

**UNITED STATES COURT OF APPEALS  
FOR THE FEDERAL CIRCUIT**

---

PRISM TECHNOLOGIES LLC,  
*Plaintiff-Cross-Appellant,*

v.

SPRINT SPECTRUM L.P., DBA SPRINT PCS,  
*Defendant-Appellant.*

---

Appeal from the United States District Court for the District of Nebraska in Case No. 8:12-cv-00123, Judge Lyle E. Strom

---

**CORRECTED NON-CONFIDENTIAL OPENING BRIEF OF  
SPRINT SPECTRUM L.P.**

---

CARTER G. PHILLIPS  
RYAN C. MORRIS  
JENNIFER J. CLARK  
SIDLEY AUSTIN LLP  
1501 K Street, N.W.  
Washington, D.C. 20005  
Telephone: (202) 736-8000  
Facsimile: (202) 736-8711

MICHAEL J. BETTINGER  
IRENE YANG  
SIDLEY AUSTIN LLP  
555 California Street, Suite 2000  
San Francisco, California 94104  
Telephone: (415) 772-1200  
Facsimile: (415) 772-7400

*Counsel for Sprint Spectrum L.P.*

---

---

## CERTIFICATE OF INTEREST

Counsel for appellant Sprint Spectrum L.P. certifies the following:

1. The full name of every party represented by me is:

Sprint Spectrum L.P.

2. The name of the real party in interest represented by me is:

None

3. All parent corporations and any publicly held companies that own 10 percent of the stock of the party or amicus curiae represented by me are listed below:

Sprint Spectrum L.P. is directly or indirectly owned by Sprint Communications, Inc. (SCI). SCI is a subsidiary of Sprint Corporation, a public company listed on the New York Stock Exchange. SoftBank Corp., a public company listed on the Tokyo Stock Exchange First Section, owns 10% or more of the stock of Sprint Corporation.

4. The names of all law firms and the partners or associates who appeared for Sprint Spectrum L.P. in proceedings before the District Court, or are expected to appear in this Court, are:

SHOOK, HARDY & BACON LLP: Albert F. Harris, B. Trent Webb, Beth A. Larigan, Christine A. Guastello, Jesse J. Camacho, John D. Garretson, Jonathan N. Zerger, Mary J. Peal, Richard D. Eisner, Sara D. Sunderland

LOCHER PAVELKA DOSTAL BRADDY & HAMMES, LLC: Amy M. Locher

CASSEM, TIERNEY, ADAMS, GOTCH & DOUGLAS: Carolyn A. Wilson, David A. Blagg, Michael K. Huffer

HILGERS GRABEN PLLC: Carrie S. Dolton, Michael T. Hilgers

K&L GATES LLP: Christopher Hanba, Margaux L. Nair, Michael J. Abernathy

SIDLEY AUSTIN LLP: Carter G. Phillips, Michael J. Bettinger, Ryan Morris, Irene I. Yang, Jennifer J. Clark

Dated: March 31, 2016

/s/ Ryan Morris  
Ryan Morris

## TABLE OF CONTENTS

Pursuant to Federal Circuit Rules 28(d)(1)(B), Appellant has prepared a public version of its brief in which it has redacted certain confidential information. Specifically, the material omitted on pages 2, 16, 17, 18, 19, 20, 22, 23, 24, 25, 26, 27, 29, 38, 39, 42, 47, 51, 52, 53, 56, 57, 58, and 67 contains references to information that has been designated confidential by the parties. Specifically, each of the pages cited above contains information that was sealed in the district court and requires continued confidential treatment in this Court.

CERTIFICATE OF INTEREST .....	i
TABLE OF CONTENTS .....	iii
TABLE OF AUTHORITIES.....	vi
STATEMENT OF RELATED CASES .....	ix
INTRODUCTION.....	1
JURISDICTIONAL STATEMENT .....	4
STATEMENT OF ISSUES.....	4
STATEMENT OF THE CASE .....	5
STATEMENT OF THE FACTS .....	6
A.    The Asserted Patents.....	6
B.    Prism's Suit Against Sprint and Other Wireless Service Providers .....	10
1.    The district court's claim construction .....	12
2.    Sprint's motion to exclude Prism's expert .....	14
3.    The first wireless service provider trial .....	16
4.    Sprint's trial and wireless system .....	16
5.    Sprint's trial and the use of AT&T's settlement .....	22

6.	Sprint’s trial and Prism’s damages theory .....	27
7.	Sprint’s post-trial motions .....	30
SUMMARY OF THE ARGUMENT .....		30
STANDARD OF REVIEW.....		35
ARGUMENT .....		36
I.	THE JUDGMENT OF INFRINGEMENT CANNOT STAND BECAUSE SPRINT’S SYSTEMS AND PROCESSES DO NOT MEET THE “INTERNET PROTOCOL NETWORK” LIMITATION. ....	36
A.	Under the District Court’s Proper Claim Construction, Sprint’s Systems and Processes Do Not Infringe the Asserted Claims. ....	36
B.	The Finding Of Infringement Resulted From Numerous Legal Errors. ....	40
1.	The district court erroneously allowed the jury to alter the “no controlling organization” requirement...	41
2.	Prism compounded the court’s error by redefining the “path to access” requirement. ....	45
II.	ADMISSION OF THE SETTLEMENT AGREEMENT BETWEEN PRISM AND AT&T VIOLATED FEDERAL RULES OF EVIDENCE 403 AND 408 AND REQUIRES A NEW TRIAL. ....	47
A.	Admission of the AT&T Settlement Violated Federal Rule of Evidence 403. ....	48
B.	Admission of the AT&T Settlement Violated Federal Rule of Evidence 408. ....	54
III.	THE DISTRICT COURT APPLIED THE WRONG STANDARD IN REVIEWING SPRINT’S POST-TRIAL MOTIONS AND UTTERLY FAILED TO CONSIDER MULTIPLE GROUNDS FOR RELIEF.....	58

IV. THE DISTRICT COURT ERRED IN ADMITTING PRISM'S COST-SAVINGS DAMAGES THEORY, WHICH FAILS TO REFLECT THE FOOTPRINT OF THE INVENTION .....	61
A. A Reasonable Royalty Must Be Closely Tied To The Footprint Of The Invention.....	61
B. Prism's Damages Expert Failed to Tie His Model to the Invention .....	63
C. Even If It Were Permissible to Measure Damages Based on the Non-Patented Backhaul, Prism's Model Nonetheless Impermissibly Departs from the Footprint of the Invention and Is Otherwise Unreliable.....	67
CONCLUSION .....	70
CERTIFICATE OF SERVICE.....	72

## TABLE OF AUTHORITIES

	<b>Page(s)</b>
<b>Cases</b>	
<i>Advanced Cardiovascular Sys., Inc. v. Medtronic, Inc.</i> , 265 F.3d 1294 (Fed. Cir. 2001) .....	35
<i>Avid Tech., Inc. v. Harmonic, Inc.</i> , 812 F.3d 1040 (Fed. Cir. 2016) .....	35
<i>Chism v. CNH Am. LLC</i> , 638 F.3d 637 (8th Cir. 2011).....	35
<i>Cordis Corp. v. Boston Sci. Corp.</i> , 561 F.3d 1319 (Fed. Cir. 2009) .....	43
<i>Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.</i> , __ F.3d __, 2016 WL 766661 (Fed. Cir. Feb. 29, 2016) .....	2, 32, 40, 43, 46, 47
<i>Georgia-Pac. Corp. v. U.S. Plywood Corp.</i> , 318 F. Supp. 1116 (S.D.N.Y. 1970) modified sub nom. <i>Georgia-Pac. Corp. v. U.S. Plywood-Champion Papers, Inc.</i> , 446 F.2d 295 (2d Cir. 1971) .....	49
<i>Gray v. Bicknell</i> , 86 F.3d 1472 (8th Cir. 1996).....	35, 60
<i>Hallmark Cards, Inc. v. Murley</i> , 703 F.3d 456 (8th Cir. 2013).....	35
<i>Kennon v. Slipstreamer, Inc.</i> , 794 F.2d 1067 (5th Cir. 1986) .....	57
<i>LaserDynamics, Inc. v. Quanta Computer, Inc.</i> , 694 F.3d 51 (Fed. Cir. 2012) .....	3, 33, 48, 49, 50, 51, 52, 54
<i>Lucent Techs., Inc. v. Gateway Inc.</i> , 580 F.3d 1301 (Fed. Cir. 2009) .....	52, 62

<i>McHann v. Firestone Tire &amp; Rubber Co.,</i> 713 F.2d 161 (5th Cir. 1983).....	57
<i>McKnight By &amp; Through Ludwig v. Johnson Controls, Inc.,</i> 36 F.3d 1396 (8th Cir. 1994).....	59
<i>Monsanto Co. v. McFarling,</i> 488 F.3d 973, 980 (Fed. Cir. 2007) .....	66
<i>In re MSTG, Inc.,</i> 675 F.3d 1337 (Fed. Cir. 2012) .....	54, 55
<i>O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.,</i> 521 F.3d 1351 (Fed. Cir. 2008) .....	1, 43, 44, 45
<i>Pioneer Hi-Bred Int'l, Inc. v. Ottawa Plant Food, Inc.,</i> 219 F.R.D. 135 (N.D. Iowa 2003).....	56
<i>Playboy Enterprises, Inc. v. Chuckleberry Pub., Inc.,</i> 687 F.2d 563 (2d Cir. 1982) .....	57
<i>ResQNet.com, Inc. v. Lansa, Inc.,</i> 594 F.3d 860 (Fed. Cir. 2010) .....	50, 61, 62, 65
<i>Riles v. Shell Expl. &amp; Prod. Co.,</i> 298 F.3d 1302 (Fed. Cir. 2002) .....	65, 66
<i>Rude v. Westcott,</i> 130 U.S. 152, 164 (1889).....	49
<i>Teva Pharm. USA, Inc. v. Sandoz, Inc.,</i> 135 S. Ct. 831 (2015).....	35, 43
<i>Uniloc USA, Inc. v. Microsoft Corp.,</i> 632 F.3d 1292 (Fed. Cir. 2011) .....	49, 62
<i>VirnetX, Inc. v. Cisco Sys., Inc.,</i> 767 F.3d 1308 (Fed. Cir. 2014) .....	62
<i>Walker v. Soo Line R. Co.,</i> 208 F.3d 581 (7th Cir. 2000).....	69

## **Statutes**

28 U.S.C. § 1295(a) .....	4
28 U.S.C. § 1331 and § 1338(a) .....	4
35 U.S.C. § 284 .....	62

## **Other Authorities**

Federal Rule of Appellate Procedure 32(a).....	71
Federal Rule of Evidence 403.....	2, 4, 30, 32, 47, 48, 54
Federal Rule of Evidence 408.....	3, 4, 30, 32, 33, 47, 48, 54, 55, 56, 57, 58

## **STATEMENT OF RELATED CASES**

No other appeal in or from the same proceeding was previously before this Court or any other appellate court.

The following related case involving the same patents in suit is currently pending in the United States District Court for the District of Nebraska:

*Prism Technologies LLC v. T-Mobile USA, Inc.*, Case No. 8:12-cv-124 (D. Neb.)

In addition, the following related cases are also pending in the United States District Court for the District of Nebraska and are currently stayed pending the outcome of this appeal and any appeal in the above-referenced *T-Mobile* case:

*Prism Technologies LLC v. U.S. Cellular Corp.*, Case No. 8:12-cv-125 (D. Neb.)

*Prism Technologies LLC v. Cellco Partnership d/b/a Verizon Wireless*, Case No. 8:12-cv-126 (D. Neb.).

These three cases were consolidated with the present case in the district court for pre-trial purposes.

In addition, this Court has previously heard two appeals involving the same or related patents:

*Prism Technologies LLC v. McAfee, Inc., et al.*, No. 2013-1135: In this appeal, a panel composed of Judges Lourie, Bryson, and O'Malley affirmed the judgment against Prism under Federal Circuit Rule 36.

*Prism Technologies LLC v. Verisign, Inc., et al.*, No. 2007-1315: In this appeal, a panel composed of Judges Mayer, Bryson, and Gajarsa affirmed the judgment against Prism under Federal Circuit Rule 36.

## INTRODUCTION

The district court committed several reversible errors leading to the judgment of infringement and award of damages in favor of Prism Technologies LLC (Prism) and against Sprint Spectrum L.P. (Sprint). These errors warrant outright reversal of the judgment or, at a minimum, a new trial.

*First*, the district court fundamentally erred by allowing Prism to argue a different claim construction to the jury than the one adopted by the court. After the court's *Markman* order construed the "Internet Protocol network" limitation, Prism's expert altered that construction in order to conclude that Sprint's systems and processes met the claim limitation. Sprint sought to exclude that testimony as inconsistent with the court's construction, but the district court ruled that the issue presented a factual question for the jury and erroneously allowed Prism to argue the altered construction to the jury. As this Court has explained, however, "the scope of the asserted claims is a question of law." *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co.*, 521 F.3d 1351, 1361 (Fed. Cir. 2008). And because it is an issue for a court, not a jury, this Court has instructed courts not to "delegat[e] to the jury the task of

determining claim scope.” *Eon Corp. IP Holdings LLC v. Silver Spring Networks, Inc.*, \_\_ F.3d \_\_, 2016 WL 766661, at \*3 (Fed. Cir. Feb. 29, 2016). Absent this fundamental legal error, the evidence showed that under the district court’s proper construction of this claim limitation, Sprint’s systems and processes do not infringe the asserted claims as a matter of law.

*Second*, the district court further erred in allowing Prism to mask the deficiencies of its case by introducing its settlement agreement with AT&T, whom Prism sued at the same time as Sprint on the same asserted patents at issue here, and who settled in the midst of trial. ■

[REDACTED] AT&T and Prism entered into a settlement agreement [REDACTED]

[REDACTED]. During Sprint’s trial, the district court—without analysis—allowed Prism to introduce evidence of this settlement and argue that it established Sprint’s liability and the baseline amount of an appropriate damages award. This was error. Under Federal Rule of Evidence 403, settlement agreements are presumptively excluded except in a narrow set of circumstances not met here. In fact, this case is resolved by this Court’s decision in

*LaserDynamics, Inc. v. Quanta Computer, Inc.*, 694 F.3d 51, 77 (Fed. Cir. 2012), which ruled that a settlement agreement under circumstances similar to those here should never have been presented to the jury. Moreover, the AT&T settlement agreement should have been excluded for the independent reason that it violates Federal Rule of Evidence 408. That Rule precludes settlement evidence to establish liability or the amount of a claim. But that is precisely why Prism introduced the AT&T settlement.

In any event, the district court's failure to apply the correct standard or analysis to Sprint's new trial motion alone warrants reversal.

*Third*, the district court erred in permitting Prism to introduce a cost-savings theory of damages that is untethered to the patented features of the asserted claims. Prism's theory based the damages on how much it would cost Sprint to build its own network for transporting data from cell towers to the Sprint data center. But the patented claims are not for a network; the untrusted network that carries data is the backdrop for the methods and systems of the asserted claims. Instead, the patents claim methods and systems for authenticating the identity

of a client computer that is requesting access to protected computer resources. Prism's theory in no way addresses the key patented features of the inventions.

The Court should reverse and vacate the award of damages.

## **JURISDICTIONAL STATEMENT**

The district court had jurisdiction under 28 U.S.C. § 1331 and § 1338(a). Following a jury verdict, the district court entered judgment on June 24, 2015. Appx1. The court granted Prism's motion for an award of pre- and post-judgment interest and entered an amended judgment on December 18, 2015. Appx14–15. Sprint filed a timely notice of appeal. Appx34267. This Court has jurisdiction under 28 U.S.C. § 1295(a).

## **STATEMENT OF ISSUES**

1. Whether the district court erred by allowing Prism to argue to the jury a different claim construction of the "Internet Protocol network" limitation from that adopted by the court.
2. Whether the district court erred by permitting Prism to introduce evidence about a co-defendant's settlement at trial in violation of Federal Rules of Evidence 403 and 408.

3. Whether the district court erred in allowing Prism to introduce a cost-savings theory that was not tied to the inventive features of the asserted claims.

## **STATEMENT OF THE CASE**

In 2012, Prism sued Sprint, alleging infringement of United States Patent Nos. 7,290,288 (the '288 patent) and 8,127,345 (the '345 patent). Appx316–20. In 2013, Prism amended its complaint to add allegations of infringement of a third patent, Patent No. 8,387,155 (the '155 patent), and later dropped the '288 patent. The patents generally claim methods and processes for a server computer to authenticate and grant permission to a client computer seeking protected computer resources over an untrusted network, such as the Internet. Appx156 ('345 patent 3:47–64). Prism's suit against Sprint was consolidated for pre-trial purposes with several other suits against wireless service providers AT&T, Verizon, T-Mobile, and U.S. Cellular.

On July 30, 2013, the district court issued its *Markman* order, construing the claims of the three patents. Appx16–83. After expert reports were exchanged, Sprint and the other defendants sought, among other things, to exclude Prism's expert for attempting to alter the

district court’s construction of certain claims. Sprint also sought summary judgment of noninfringement. The district court denied both motions and set the cases for separate trials. Appx21870–77; Appx102–07.

Sprint’s case was tried to a jury in Omaha, Nebraska in June 2015 on claims 1 and 33 of the ’345 patent and claims 7 and 37 of the ’155 patent. The jury returned a verdict of infringement for Prism, Appx23484–85, and the district court entered judgment on June 24, 2015, Appx1. The district court denied Sprint’s post-trial motions, Appx2–6, denied Prism’s request for fees (before Prism even filed its reply), Appx28842–43, denied Prism’s request for an ongoing royalty, Appx11–13, and granted Prism’s motion for an award of pre- and post-judgment interest, Appx11. Sprint timely appealed, Appx34267–34271, and Prism cross-appealed. Appx34277–34279.

## **STATEMENT OF THE FACTS**

### **A. The Asserted Patents**

Prism initially developed custom software and systems for the financial services industry, Appx26397 (Tr. 103:12–14), but in approximately 2003, it emerged from bankruptcy with the sole focus of licensing patents and enforcing its intellectual property through

litigation, Appx26415–16 (Tr. 121:17–122:2); Appx27085–87 (Tr. 662:10–664:8); Appx27194–95 (Tr. 731:24–732:5); Appx27196–97 (Tr. 733:25–734:3); Appx40050 (TX 1404 at 37:01–10). Among that intellectual property are the ’345 and ’155 patents.

The technology at issue in these patents generally relates to security for transactions occurring over certain types of computer networks. Appx155 (’345 patent 1:15–16). The purpose of these inventions was to improve upon other systems that allow businesses to provide transaction services (*e.g.*, e-commerce) to those connected to the Internet or another type of untrusted network. *Id.* (’345 patent 1:20–56); Appx223 (’155 patent 1:20–56). In particular, the inventions involve systems and methods for controlling access to protected computer resources provided over an untrusted network, such as the Internet. Appx110 (’345 patent Abstract); Appx155 (’345 patent 1:16–19); Appx177 (’155 patent Abstract).

The inventions generally involve a client-server system communicating over an untrusted network in which the server computer secures and tracks “usage of transaction services or computer resources by a client computer,” Appx155 (’345 patent 1:60–62), and

permits the client computer to access protected resources after authenticating the client computer's identity, *id.* ('345 patent 1:60–2, 1:63–2:21). In this system and method, the server has a clearinghouse that stores the identity data of both the client and server computers. The client computer runs software that, at the start of an operation, is programmed to forward its identity data to the server. The clearinghouse on the server is adapted to authenticate the identity of the client computer in response to the client's request and to permit access to the protected resource upon successful authentication of the client and server. *Id.* ('345 patent 1:62–2:21).

Claim 1 of the '345 patent is representative of the asserted method claims at issue. It claims

A method for controlling access, by at least one authentication server, to protected computer resources provided via an Internet Protocol network, the method comprising:

receiving, at the at least one authentication server from at least one access server, identity data associated with at least one client computer device, the identity data forwarded to the at least one access server from the at least one client computer device with a request from the at least one client computer device for the protected computer resources;

authenticating, by the at least one authentication server, the identity data received from the at least one access server, the identity data being stored in the at least one authentication server;

authorizing, by the at least one authentication server, the at least one client computer device to receive at least a portion of the protected computer resources requested by the at least one client computer device, based on data associated with the requested protected computer resources stored in at least one database associated with the at least one authentication server; and

permitting access, by the at least one authentication server, to the at least the portion of the protected computer resources upon successfully authenticating the identity data and upon successfully authorizing the at least one client computer device.

Appx171 ('345 patent 34:17–42).

Claim 1 of the '155 patent is representative of the asserted system claims at issue. It claims:

A system for controlling access to protected computer resources provided via a network utilizing at least one Internet Protocol, the system comprising:

at least one authentication server having an associated database to store (i) identity data associated with at least one client computer

device, and (ii) data associated with said protected computer resources;

at least one access server adapted to receive said identity data from said at least one client computer device;

said at least one access server adapted to forward said identity data received from said at least one client computer device to said at least one authentication server;

said at least one authentication server adapted to authenticate said identity data responsive to a request for said protected computer resources by said at least one client computer device;

said at least one authentication server adapted to authorize said at least one client computer device to receive at least a portion of said protected computer resources, based on said stored data associated with said protected computer resources; and

said at least one authentication server adapted to permit access to said at least a portion of said protected computer resources upon successfully authenticating said identity data and upon successfully authorizing said at least one client computer device.

Appx239 ('155 patent 34:27–52).

## **B. Prism's Suit Against Sprint and Other Wireless Service Providers**

The '345 patent issued to Prism in February 2012, and shortly thereafter, Prism filed suit against Sprint. Prism alleged that Sprint's

wireless networks allow computer devices, such as smartphones, to access protected computer resources using the methods and systems claimed by Prism's patents. Appx1848 (¶ 11). Prism claimed that Sprint's wireless networks and data services—including its 3G, 4G LTE, and 4G WiMax systems<sup>1</sup>—implemented authentication systems and methods so that only authorized devices may access a portion of the networks or services. Appx1849–51 (¶¶ 18–29). According to Prism, Sprint's wireless networks and data services infringed claims of the '288 and '345 patents.<sup>2</sup>

At the same time that Prism sued Sprint, Prism also brought suit against other wireless service providers: AT&T, T-Mobile, Verizon, and U.S. Cellular. Appx316; *Prism Techs. LLC v. AT&T, Inc.*, No. 8:12-CV-122 (D. Neb.); *Prism Techs., LLC v. T-Mobile USA, Inc.*, No. 8:12-CV-124 (D. Neb.); *Prism Techs. LLC v. United States Cellular Co.*, No. 8:12-CV-125 (D. Neb.); *Prism Techs. LLC v. Cellco Partnership d/b/a Verizon Wireless*, No. 8:12-CV-126 (D. Neb.). Sprint and the other

---

<sup>1</sup> Those systems are based on third generation (3G) code division multiple access (CDMA) technology, fourth generation (4G) services using Worldwide Interoperability for Microwave Access (WiMAX), and 4G services utilizing Long Term Evolution (LTE) technology.

<sup>2</sup> Prism later dropped the '288 patent.

wireless service providers were treated as co-defendants throughout the pre-trial phase of the case; the cases were consolidated for all pre-trial purposes; and Prism took the position that the cases should be consolidated for trial. Appx1454, 1461–62. In 2013, when the '155 patent issued, Prism amended its complaint to include allegations that Sprint and the other defendants infringed claims of this patent.

*Compare* Appx317–18 (1st Complaint 2–3), *with* Appx1847–48 (2nd Am. Complaint 2–3).

## **1. The district court’s claim construction**

During pre-trial proceedings, Prism and the various defendants stipulated to the construction of numerous terms in the asserted claims. Appx81. They also stipulated that “the preambles of the asserted claims are limiting.” Appx82. Relevant here, however, the parties disputed the construction of the term “Internet Protocol network” in the preambles’ limitation that the claimed method and system control access to “protected computer resources provided via an Internet Protocol network.” Appx171 ('345 patent 34:17–19).<sup>3</sup>

---

<sup>3</sup> The '345 patent uses the phrase “Internet Protocol network,” whereas the '155 patent uses the phrase “network utilizing at least one Internet Protocol.” The district court and parties have not differentiated

As the district court explained, the parties essentially agreed that the phrase “Internet Protocol network” means at least a “*network* using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, and HTTP/IP.” Appx28–29 & n.4 (emphasis added).<sup>4</sup> The dispute between the parties centered on the type of “*network*” required and whether it must be “untrusted.” The defendants argued “that the ‘Internet Protocol network’ terms as used in the asserted patents’ claims should be restricted to untrusted networks.” Appx29. And while “Prism concede[d]” that the inventions generally claim systems “for controlling the operation and access to protected resources where the access server and client computer communicate *over an untrusted network*,” it maintained that the inventions are not limited to untrusted networks. *Id.* (emphasis added).

After reviewing the claim language, specification, and prosecution history, including Prism’s disclaimers to the PTO, the district court

---

between these phrases and have given them the same meaning. Appx27.

<sup>4</sup> The only difference on this aspect of the construction was Sprint’s proposal that the claim requires HTTP/IP, whereas Prism proposed merely HTTP. The district court adopted both HTTP and HTTP/IP. Appx29 n4.

concluded that the term “Internet Protocol network” is indeed limited to untrusted networks. Appx30–44. The court further adopted verbatim the explicit definition of “untrusted” found in the specifications “where untrusted is defined as a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous.” Appx45; *see* Appx156 ('345 patent 3:49–52); Appx224 ('155 patent 3:49–52).

## **2. Sprint’s motion to exclude Prism’s expert**

After the parties exchanged expert reports, Sprint and the other defendants jointly sought to exclude, in part, the testimony of Prism’s expert, John Minor, as an impermissible attempt to revise the court’s construction of the “Internet Protocol network” limitation. Sprint and the other defendants argued that Minor’s testimony improperly attempted to revise the district court’s construction by modifying the definition of an untrusted network to require no “single” controlling organization, as opposed to the court’s requirement that there be “no controlling organization.” As the court explained, Minor’s report disclosed that his opinion at trial would be that the defendants’ systems satisfy the “Internet Protocol network” limitation because, according to

Minor, the district court construed the term “to mean in part ‘a public network with no *single* controlling organization.’” Appx88. Indeed, the court included the following visual representation of Minor’s interpretation that shows his addition of the word “single” in the court’s construction:

Minor’s interpretation	The Court’s <i>Markman</i> order
<p>“a public network with no single controlling organization, with the path to access the network being undefined and the user being anonymous.”</p>	<p>“a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous.”</p>

Appx91.

The district court denied the motion, however, by concluding that the issue was one of fact for the jury. According to the court, the question is essentially whether the “defendants’ networks, over which each exert[s] an arguable level of control, can likewise constitute a public, uncontrolled, undefined pathway, anonymous-user internet like the aggregate internet.” Appx94. The court reasoned that the question boils down to whether “an organization exert[s] sufficient control over its network” to be considered “trusted.” *Id.* The court thus ruled that this “is a question of fact” for the jury and that Minor could rely on his “interpretation” at trial. *Id.*

### **3. The first wireless service provider trial**

Although Prism took the position that the separate cases against all the wireless service providers should be consolidated for trial, Appx1461–62, the cases were eventually tried separately. AT&T was the first to go to trial, which commenced on October 14, 2014. [REDACTED]

[REDACTED] Prism and AT&T entered into a settlement agreement. Appx27148 (Tr. 685). Under the agreement, AT&T paid Prism [REDACTED]

### **4. Sprint's trial and wireless system**

After AT&T's settlement, Sprint became the next wireless service provider to go to trial. At trial, the facts establishing Sprint's systems and processes for a wireless user's phone to be authenticated and to access protected resources in Sprint's data center were undisputed. A cellular phone on one of Sprint's accused 3G, 4G LTE, or 4G WiMAX networks immediately recognizes a Sprint cell tower. Appx26360 (Tr. 66:23–24). The phone communicates with the Sprint antenna on the nearest cell tower at a proprietary radio frequency that the FCC has

dedicated to Sprint, and the phone's transmission carries with it information about the user. Appx27330 (Tr. 867:14–19); Appx27332 (Tr. 869:10–14, 22–24); Appx27607 (Tr. 1144:15–19). The radio signal is then converted into a digital signal and is sent from the antenna to a Sprint base station [REDACTED] Appx27332–33 (Tr. 869:24–870:22).

The signal then passes from the Sprint base station to the entry point for an Ethernet backhaul [REDACTED] Appx27347 (Tr. 884:1–25); Appx27407 (Tr. 944:13–25). An Ethernet backhaul is a “data transport service” for large businesses or communications carriers within a particular geographic region. Appx38184 (explaining that the “Ethernet is a Layer 2 data transport service that offers enterprise and Carrier customers the ability to interconnect standard 10/100/1000 Mbps Local Area Network (LAN) interfaces within a metropolitan area”). Sprint does not own or operate the Ethernet backhauls; instead, Sprint has entered into contracts with [REDACTED] third-party providers, sometimes referred to as “alternative access vendors” or AAVs, who each provide an Ethernet backhaul, and each of whom owns, operates, and controls the Ethernet backhaul that it provides to Sprint.

Appx26535 (Tr. 72:19–22); Appx26929, 26932–33 (Tr. 466:14–21; 469:22–470:2); Appx26948 (Tr. 485:1–5) (“each one of the AAV networks, are owned and operated and controlled by themselves individually”); Appx26948–49 (Tr. 485:17–486:1); Appx27314 (Tr. 851:1–2).

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Appx27040–41 (Tr. 577:19–578:3); Appx27039–40 (Tr. 576:23–577:6); Appx40033; Appx38197, 38199; Appx27452–53 (Tr. 989:23–990:15); Appx27430–31 (Tr. 967:18–968:2); Appx27450–52 (Tr. 987:22–989:13). [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Appx27432–33 (Tr. 969:23–970:18);

Appx27046 (Tr. 583:14–20); Appx27048 (Tr. 585:5–7), [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

Similarly undisputed were the facts establishing the other accused Sprint systems, which include femtocells, picocells, and outbound roaming, and [REDACTED]

[REDACTED] See Appx27547 (Tr. 1084:9–18); Appx27548 (Tr. 1085:7–16); Appx27558 (Tr. 1095:3–10).<sup>5</sup> A femtocell or picocell essentially replaces the cell tower-base station combination used in the vast majority of Sprint’s accused systems. Appx26906–07, 26908–09, 26918 (Tr. 443:24–444:11, 445:19–446:2, 455:13–14). That is, radio signals containing data about a user’s identity are transmitted from the cell phone to the femtocell or picocell device, where they are converted into digital signals. Appx27555 (Tr. 1092:16–24); Appx26704 (Tr. 241:13–22). [REDACTED]

---

<sup>5</sup> Although Prism accused these other systems of infringement, it did not assert any damages based on them. In any event, these systems do not infringe the asserted patents.

At trial, a primary dispute between Sprint and Prism was whether Sprint’s system and processes meet the “Internet Protocol network” limitation—that is, whether protected computer resources are “provided via an Internet Protocol network.” Appx171 (’345 patent 34:18–19); Appx239 (’155 patent 34:28) (system requiring computer resources “provided via a network utilizing at least one Internet Protocol”). Prism’s theory at trial was that the only aspect of Sprint’s system that meets this limitation is the Ethernet backhaul over which user data is carried from the base station to the Sprint data center.

Appx26906 (Tr. 443:1–5); Appx26925 (Tr. 462:14–24); Appx26927–29 (Tr. 464:16–466:8); Appx26937–38 (Tr. 474:18–475:2); Appx26942 (Tr. 479:17–24); Appx26943 (Tr. 480:3–6). Prism did not contend that the limitation was met by the process leading to the base station or Sprint’s data center. Appx27668–69 (Tr. 1205:16–1206:25); Appx27670 (Tr. 1207:15–25) (acknowledging that Prism is “not accusing” the data center, “which has to be secure and private” and is “not accusing the base stations.”). The “Internet Protocol network,” in Prism’s view, is the backhaul. Consistent with the position taken in Minor’s expert report, Prism argued to the jury that the asserted claims required no “*single* controlling organization” and that the Ethernet backhaul satisfied this element because no single organization controlled *all* of the backhauls, even though an Ethernet backhaul provider owns, operates, and controls its individual backhaul (and even though Sprint controls the data that goes into the backhaul and is the only one who can unpack it on the other end). Appx26948–49 (Tr. 485:19–486:1) (emphasis added); *see* Appx39965 (asking whether “there’s no single AAV that basically runs the whole backhaul network”). Prism also asserted that the “path through the network” is undefined in Sprint’s system and that therefore

Sprint's system satisfies another element of the district court's definition of "untrusted," which requires that the "path to access the network is undefined." See Appx26950–26951 (Tr. 487:24–488:25); Appx26950–26953 (Tr. 487:16–490:5); Appx26984 (Tr. 431:9–25). Although the path for a user's phone to access a particular backhaul is defined (*i.e.*, cell phone to cell tower, to base station, to backhaul), Prism argued that as a user travels, the user's signal will be sent to different cell towers, and thus the path "through" the network is undefined. *Id.*

### **5. Sprint's trial and the use of AT&T's settlement**

In response to Sprint's undisputed evidence of its systems and processes, Prism sought to introduce evidence of AT&T's Settlement Agreement. Prior to trial, Sprint moved to preclude Prism from presenting testimony regarding this agreement. Appx19351. Sprint explained that under this Court's precedent, relying on such agreements to establish reasonable royalty damages is impermissible absent certain limited circumstances that are inapplicable here.

[REDACTED]

[REDACTED]

[REDACTED] than any other Prism [REDACTED]

[REDACTED] agreement; was negotiated two and a half years after the hypothetical negotiation at issue here; was executed well into the AT&T trial [REDACTED]  
[REDACTED]; and—particularly because AT&T was essentially Sprint’s co-defendant with regard to the patents in suit—created a high risk of undue prejudice from treating the settlement as evidence that Sprint infringes. The district court denied Sprint’s motion with no analysis or discussion of the parties’ arguments or this Court’s precedents, stating without elaboration “Denied.” Appx105.

Throughout the Sprint trial, Prism repeatedly invoked the AT&T Settlement Agreement. After describing the history of the asserted patents, Prism’s opening statements turned immediately to the AT&T Settlement Agreement and linked it to Sprint’s liability in this case. Prism’s counsel stated: “While this case [against Sprint] is going on, ... AT&T ... took a license to Prism’s patents. And the judge told you that there’s going to be a lot of money at stake here and there is.”

Appx26358–26359 (Tr. 64–65). He continued: “AT&T got a huge discount on their license because they didn’t wait for a jury verdict.”

Appx26359 (Tr. 65). [REDACTED]

[REDACTED] Prism's counsel emphasized “[w]e're not going to offer a discount to Sprint.” *Id.* Prism's counsel wrapped up his opening argument by again emphasizing that AT&T paid [REDACTED] and that “[w]e're going to ask for more than double that from Sprint.” Appx26370 (Tr. 76).

On direct examination of Prism's president and chief financial officer, Mr. Duman, who testified as a fact witness, Prism's counsel again invoked the AT&T Settlement Agreement. Responding to the question whether Prism has “any licenses to the '155 and '345 patents with a wireless carrier,” Duman testified that Prism had a license with AT&T for which AT&T paid [REDACTED]. Appx27145 (Tr. 682). Prism's counsel then elicited testimony equating AT&T's and Sprint's “activity” with regard to the asserted patent claims. Duman testified that the license came about when Prism was “involved with litigation with AT&T *on the same patents for essentially the – the same activity* and we – we got to trial, and we were in trial or – or right at the beginning of trial and [REDACTED]” Appx27146 (Tr. 683) (emphasis added). Prism's counsel went on to highlight the timing of the agreement, asking “I think you mentioned it was during the

Prism/AT&T trial; is that correct?” Appx27148 (Tr. 685). When Duman responded that the Settlement was signed [REDACTED]

[REDACTED] Duman then elaborated that the agreement was signed shortly [REDACTED]

[REDACTED] Duman also testified that the [REDACTED] was “a discounted amount,” *id.*, and discussed the terms of the Settlement at length, Appx27148–27154 (Tr. 685–91).

Prism again linked Sprint’s and AT&T’s activities with regard to the asserted claims, with Prism’s counsel asking Duman, over Sprint’s objection, how Prism “view[s] the use of the asserted patents by AT&T when compared to the use of the asserted patents by Sprint.” Appx27155 (Tr. 692). Duman once again equated AT&T and Sprint: “the application is very similar … they use it to help authenticate the smartphone devices to whatever resources they’re wanting access to” and “both companies are … large companies” with “millions of subscribers who are authenticated thousands of times every year and so a lot of similarities in that regard.” Appx27155–56 (Tr. 692–93). When

asked about the basis for his “understanding regarding the use of the asserted patents by Sprint and AT&T,” Duman again emphasized that AT&T and Sprint were the same: “When we first evaluated the – the wireless application that these two wireless carriers may have been using, we did do levels of investigation in terms of – of how they might be using it.” Appx27156 (Tr. 693).

Prism’s refrain that Sprint and AT&T were equally liable and AT&T’s settlement was the benchmark for the damages Sprint owed to Prism did not stop there. Prism’s expert witness, Mr. Malackowski, also testified at length about the settlement. Appx27233–34 (Tr. 770–71, 784–793). And in closing, Prism’s counsel again argued [REDACTED] [REDACTED] Appx24933 (Tr. 1470). He once again portrayed the AT&T Settlement as indicative of Sprint’s liability and suggested Sprint should pay more for going to trial. Appx27933–34 (Tr. 1470–71). Finally, he endorsed the AT&T Settlement—[REDACTED]—as the appropriate measure of damages for Sprint’s use of the two asserted patents, stating “Trust me, I was in this courtroom with AT&T.” Appx27935 (Tr. 1472).

The jury returned a verdict for Prism in the amount of \$30 million, [REDACTED]

## **6. Sprint's trial and Prism's damages theory**

To support its damages request, Prism relied on a cost-savings theory of damages after the district court threw out Prism's initial damages theory. After receiving the first report of Prism's damages expert, Malackowski, Sprint and the other wireless carrier defendants moved to exclude his testimony as unreliable and not tied to the footprint of the invention. Appx11142. The district court granted the motion, finding Malackowski's theory "over broad and beyond the context of the invention," "methodically flawed," and "unsound." Appx13093.

After Prism settled with AT&T, Prism sought and received permission to file new expert reports. Appx13378–85. Sprint and the other defendants again moved to exclude this testimony, explaining that Malackowski should not be allowed to testify regarding the AT&T Settlement Agreement because the settlement, reached in the midst of trial, is not probative of what Sprint or the other defendants would have agreed to in a hypothetical negotiation, and its admission would be

highly and unfairly prejudicial. Appx17629. The defendants further explained that Malackowski's royalty base is not the product of sufficient facts or a reliable methodology and is not tied to the footprint of the patented invention.

In particular, Sprint and others explained that although the patented invention relates to a method of authenticating users over a public network, Malackowski failed to ground the royalty base in the incremental value of that authentication system over prior art authentication systems, but instead used the entirety of a defendant's backhaul leasing costs as his base. Sprint and the defendants noted that Malackowski acknowledged that defendants could avoid infringement by using an alternative authentication method (while continuing to lease backhaul). Yet, Malackowski did not look to any prior art authentication methods to see how much more expensive they were (if at all) than the allegedly infringing methods, but instead calculated cost savings based on the difference between a hypothetical scenario in which each defendant had to build or buy its own backhaul network, and the actual costs it incurred from leasing a backhaul network. Malackowski further departed from the footprint of the

invention by failing to determine the cost of building a new network, and instead estimating such costs based on a defendant's actual expenditures for *leasing* backhaul services. This approach improperly based the royalty on the [REDACTED] that each carrier spends to lease backhaul, including all of the features and technologies of that backhaul that have nothing to do with the patented invention, including costs for the time to repair data transmission failures, the time it takes the system to recover from an overload, the timeliness of vendor reports on network performance, and volume discounts.

The district court denied the *Daubert* motion with no analysis. See Appx95–101. The court merely summarized the parties' positions, set forth general standards for admissibility of expert damages testimony, and stated: “After review of the filings, oral arguments, and relevant case law, the Court will deny the Carrier Defendants' motions.” Appx101. At trial, Prism presented Malackowski's cost-saving damages theory to the jury, basing damages on the supposed cost to Sprint to build its own backhaul network compared to leasing backhaul services from its various providers.

## **7. Sprint’s post-trial motions**

After trial, Sprint moved for judgment as a matter of law and for a new trial on multiple grounds, including that the court erred by allowing Prism to submit a new claim construction to the jury, that admission of the AT&T Settlement evidence violated Federal Rules of Evidence 403 and 408, and that the court erred in allowing Prism’s cost-savings theory. Appx23876. The district court denied the motion, without hearing argument, and provided no analysis of the issues raised by Sprint. Indeed, with respect to the new trial motion, the court still refused to address any of this Court’s precedents on the admissibility of settlement agreements. Appx2–6. The court stated only: “After reviewing [the] facts, evidence, and the relevant law, the Court cannot say that the jury’s verdict was against the great weight of the evidence. Therefore, the Court will deny the defendant’s motion for new trial.” Appx5.

## **SUMMARY OF THE ARGUMENT**

The district court committed several legal errors—most of which occurred without analysis—that each warrant reversal.

I. The district court fundamentally erred by allowing Prism to argue a different claim construction to the jury than the one adopted by the court. Sprint’s systems and processes do not meet the “Internet Protocol network” limitation under the district court’s *Markman* order, which construed the limitation to require an untrusted network, defined (as in the patents themselves) as a “public” network with “no controlling organization” and for which the “path to access the network” is undefined. An Ethernet backhaul—which Prism claimed was the element that satisfied this limitation—has a “controlling organization,” namely the AAV backhaul provider. The Ethernet backhaul is also private, not public—Sprint contracts with each backhaul provider for a dedicated connection to carry its data. Finally, the “path to access” a backhaul is “defined” on Sprint’s system. The Ethernet backhaul thus fails to meet the “Internet Protocol network” limitation as construed by the court.

Prism avoided this evidence by offering a different construction of the “Internet Protocol network” limitation that deviated from the district court’s definition of an untrusted network. Specifically, with the district court’s permission, Prism argued that a backhaul meets the

limitation because the backhauls collectively have “no *single* controlling organization.” This fundamentally altered the court’s construction, which was based on the explicit definition in the patents’ specifications that an untrusted network is one with “no controlling organization,” not “no *single* controlling organization.” The court erred in allowing Prism to present a different construction to the jury, one that changed the scope of what is required for an untrusted network. Such a “delegation to the jury [of] the task of determining claim scope” was reversible error. *Silver Spring Networks*, 2016 WL 766661, at \*3.

Prism compounded the error by also altering the limitation element that the “path to access the network” be undefined, changing it instead to require that the “path *through* the network” be undefined. This too changed the scope of the claim requirements and should not have been delegated to the jury.

II. This Court should also reverse the judgment because the district court erred in allowing Prism to introduce the AT&T Settlement. Admitting this evidence violated Rules of Evidence 403 and 408. *First*, admission of the AT&T Settlement violated this Court’s Rule 403 precedent, under which settlements are presumptively excluded as

overly prejudicial except in narrow circumstances. Those circumstances are simply not met here. Indeed, this case is on all fours with the Court's decision in *LaserDynamics*, in which the Court concluded that under materially similar circumstances as those here, admission of a settlement agreement constituted reversible error.

*Second*, admission of this evidence independently violated Rule 408 which bans the use of settlements to show liability or the amount of damages. Prism offered the AT&T Settlement to prove precisely what 408 forbids: Prism equated Sprint's and AT&T's activities as they relate to the asserted claims and argued to the jury that AT&T's settlement amount should form the baseline of damages against Sprint. In fact, Prism suggested that Sprint should be penalized for proceeding to trial, rather than settling like AT&T. These errors at a minimum warrant a new trial.

III. Aside from these independent substantive grounds for reversal, the Court should also reverse because the district court applied the wrong standard to Sprint's new trial motion. Instead of addressing the seven legal errors raised by Sprint, the district court treated Sprint's motion as solely a sufficiency of the evidence challenge.

The court overlooked entirely the fact that “legal errors at trial” are separate bases for a new trial in the Eighth Circuit.

IV. Finally, a new trial on damages is warranted, even if the Court does not reverse on the merits. Prism’s cost-savings theory of damages was not based on the footprint of the invention, which concerns authentication of user access to protected computer resources. Rather, Prism’s theory was based on replacing each Ethernet backhaul with a Sprint built or operated backhaul. The patented invention, however, is not a network, Ethernet, or Internet. The network is the *backdrop* for the patented invention. By basing its damages calculation on the replacement cost of a backhaul rather than the patented authentication method or system, Prism’s theory is untethered to the footprint of the invention. And even if the damages theory were permissible—and it is not—the theory is otherwise unreliable. Prism’s expert calculated the supposed cost savings for building a backhaul system on another technical expert’s vague and baseless speculation derived from Sprint’s actual expenditures for leasing backhaul services, including services unrelated to the cost of building a new backhaul.

## **STANDARD OF REVIEW**

This Court reviews *de novo* the ultimate construction of a patent claim, as well as any construction based solely on intrinsic evidence.

*Teva Pharm. USA, Inc. v. Sandoz, Inc.*, 135 S. Ct. 831, 839–40 (2015).

The Court also reviews *de novo* judgment-as-a-matter-of-law determinations, “asking, as the district court did, whether only one answer to that question is reasonable given the evidence admitted at trial.” *Avid Tech., Inc. v. Harmonic, Inc.*, 812 F.3d 1040, 1045 (Fed. Cir. 2016). The Court reviews a district court’s denial of a new trial motion according to regional circuit law. *Advanced Cardiovascular Sys., Inc. v. Medtronic, Inc.*, 265 F.3d 1294, 1308 (Fed. Cir. 2001). The Eighth Circuit reviews the denial of a motion for a new trial for a clear abuse of discretion. *Hallmark Cards, Inc. v. Murley*, 703 F.3d 456, 462 (8th Cir. 2013); *Chism v. CNH Am. LLC*, 638 F.3d 637, 640 (8th Cir. 2011). In the Eighth Circuit, a new trial is warranted when a miscarriage of justice arises from (1) “a verdict against the weight of the evidence,” (2) “an excessive damage award,” (3) or “legal errors at trial.” *Gray v. Bicknell*, 86 F.3d 1472, 1480 (8th Cir. 1996).

## ARGUMENT

### **I. THE JUDGMENT OF INFRINGEMENT CANNOT STAND BECAUSE SPRINT'S SYSTEMS AND PROCESSES DO NOT MEET THE "INTERNET PROTOCOL NETWORK" LIMITATION.**

Under the district court's proper construction of the "Internet Protocol network" limitation, Sprint's accused systems and processes cannot infringe the asserted claims as a matter of law. The district court erred by allowing Prism to alter the established claim construction in this case. The judgment should be reversed.

#### **A. Under the District Court's Proper Claim Construction, Sprint's Systems and Processes Do Not Infringe the Asserted Claims.**

The district court authoritatively and correctly construed the limitation "Internet Protocol network" to mean "an untrusted network using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, HTTP, and HTTP/IP." Appx45 (claim construction order 30). The court further concluded—based on the explicit definition in the specifications—that the term "untrusted" has three specific requirements: it must be (1) "a public network with no controlling organization," (2) "with the path to access the network being undefined," (3) "and the user being anonymous." *Id.*

Prism claimed that the element of Sprint’s system that meets the “Internet Protocol network” limitation is the Ethernet backhaul, each of which is owned and operated by a third-party, and which carry the user signal from a Sprint base station to the data center. *See Appx26943* (Tr. 480:3–6) (identifying “the AAVs that Sprint uses for its backhaul” as the “Internet Protocol network”); *Appx26906* (Tr. 443:1–5); *see also Appx26937–38* (Tr. 474:13–475:2); *Appx26942, 26936–42* (Tr. 479:17–24, 473:3–479:24); *Appx26927–29, 26925* (Tr. 464:16–466:8, 462:14–24); *Appx26949–55* (Tr. 486:1–492:7); *Appx26943* (Tr. 480:12–15); *Appx26507–09* (Tr. 44:18–46:7); *Appx26895* (Tr. 432:15–25); *Appx26959* (Tr. 496:5–22).

The evidence established, however, that an Ethernet backhaul does not meet the court’s correct construction of this limitation for at least two reasons: (1) each Ethernet backhaul is private and has a controlling organization, and (2) the path to access an Ethernet backhaul *is* defined. Accordingly, Sprint’s systems do not infringe the asserted claims.

*First*, the undisputed evidence established that each Ethernet backhaul, and every part of each Ethernet backhaul, is controlled and

managed by the provider of that backhaul. Minor, Prism's own expert, admitted that “[e]ach of these networks are owned and operated by the individual organization, each one of the AAV networks, are owned and operated and *controlled by themselves individually.*” Appx26948 (Tr. 485:1–5) (emphasis added); *see also* Appx26948–49 (Tr. 485:17–486:1); Appx27314 (Tr. 851:1–2) (“The AAV networks are under the control of the AAVs.”). Because each Ethernet backhaul has a controlling organization, this limitation is not met.

Moreover, the evidence established that each backhaul is private. As evidenced by Sprint’s contracts with each backhaul provider, access to the Ethernet backhaul upon which Sprint’s data travels is not public; it is privately owned and access is restricted. Further, Sprint’s contracts with these backhaul providers ensured that Sprint had [REDACTED]

[REDACTED]

[REDACTED]

[REDACTED] Appx27452–53 (Tr. 989:23–990:15);

Appx27430–31 (Tr. 967:18–968:2); Appx27432–33 (Tr. 969:23–970:18).

[REDACTED]

[REDACTED] Minor admitted that a “trusted private

network” would consist of “a dedicated connection between Sprint’s tower” and Sprint’s data center. Appx26925 (Tr. 462:13); Appx27050 (Tr. 587:13–15). [REDACTED]

[REDACTED] Under the district court’s claim construction, each backhaul cannot be an untrusted network, and Sprint’s system and processes do not infringe.

*Second*, the evidence also established that the path to access an Ethernet backhaul on Sprint’s system is always defined. A user’s cell phone sends a radio signal to the nearest Sprint cell tower at an FCC dedicated frequency. Appx27330 (Tr. 867:14–19); *see also* Appx27332 (Tr. 869:10–14, :22–24); Appx27607 (Tr. 1144:15–19); Appx27530-31 (Tr. 1067:24–1068:10); Appx26699 (Tr. 236:8–17). That radio signal is converted into a digital signal and is sent to the Sprint base station.

Appx27332–33 (Trial Tr. 869:24–870:22). [REDACTED]

[REDACTED]  
Appx27347 (Tr. 884:1–25); Appx27407 (Tr. 944:13–25).

The undisputed evidence is that this well-defined path is the only one on Sprint’s system for a user’s data to access an Ethernet backhaul. There is no other. Appx27333–35 (Tr. 870:23–872:15) (“Q. Is that path

defined? A. Oh, yes.”); Appx27406 (Tr. 943:14–23); Appx27646 (Tr. 1183:3–12); Appx27649 (Tr. 1186:13–17). Nor did Prism contend that a backhaul is accessed through any other path on Sprint’s system.

The evidence shows that Sprint’s systems and processes do not meet the “Internet Protocol network” limitation under the district court’s proper construction of that phrase, and no reasonable jury could conclude otherwise based on the evidence.

#### **B. The Finding Of Infringement Resulted From Numerous Legal Errors.**

Prism did not challenge the facts establishing how Sprint’s systems and processes operate. Instead, Prism, with the district court’s acquiescence, offered a vastly different claim construction to the jury. This was error, and independently warrants a new trial. However, in light of the undisputed evidence of how Sprint’s systems and processes operate, *see supra* 36–40, this error requires reversal. *Silver Spring Networks*, 2016 WL 766661, at \*5 (concluding that remand for a new trial is inappropriate “because, when the claim terms are properly construed, no reasonable jury could have found that Silver Spring’s electric utility meters infringe”).

1. **The district court erroneously allowed the jury to alter the “no controlling organization” requirement.**

The district court erred by allowing Prism to argue an alternative claim construction for the “Internet Protocol network” limitation to the jury, namely that the “untrusted network” element requires “no *single* controlling organization” instead of the court’s construction of “no controlling organization.”

After Prism’s expert Minor submitted his report in this case, Sprint and the other defendants sought to exclude his testimony as inconsistent with and an obvious attempt to change the district court’s claim construction. As Sprint and others explained, Minor’s theory was that Sprint’s system satisfied the claim limitation because “there is no *single* controlling organization,” even if an individual backhaul is controlled by that backhaul’s provider. Appx92. As the district court’s own illustration of the argument showed, this theory modified the district court’s claim construction by inserting the word “single” into the court’s requirement that there be “no controlling organization.” Appx93. However, the district court concluded that the dispute boiled down to a

“question of fact” concerning the level of control over a backhaul and allowed Prism to present it to the jury. Appx94.

At trial, Prism indeed presented a different claim construction to the jury than the one adopted by the court. Prism argued to the jury that the “no controlling organization” element was met because no *single* organization controlled all of the Ethernet backhauls. Appx27926 (Tr. 1463:4–14). In particular, Prism relied on testimony that “[t]here’s no controlling organization on the *collective basis* of” the [REDACTED] [REDACTED] even if “[o]n the individual basis,” an Ethernet backhaul provider does control its backhaul. *Id.* (emphasis added). Prism’s expert testified to this theory, opining that each backhaul “control[s its] own piece but there’s not a *single* controlling organization” for *all* of the backhauls. Appx26948–49 (Tr. 485:23–486:1) (emphasis added); *see also* Appx27479–80 (Tr. 1016:25–1017:4 (Prism’s counsel inserting “no single organization” into questioning); Appx27480 (Tr. 1017:11–13) (same); Appx39965 (English Dep. Clip 58–59) (same). In other words, in order to present an infringement theory, Prism argued to the jury a different claim construction than the one adopted by the district court, one that required a different limitation (“no single

controlling organization”) than the court’s construction (“no controlling organization”). The district court erred in characterizing that claim construction issue as a “question of fact” and permitting Prism to present it to the jury.

Claim construction is a legal issue “exclusively” for ‘the court’ to determine.” *Teva Pharm. USA*, 135 S. Ct. at 835. And this Court has explicitly “held that it is improper to argue claim construction to the jury because the ‘risk of confusing the jury is high when experts opine on claim construction.’” *Cordis Corp. v. Boston Sci. Corp.*, 561 F.3d 1319, 1337 (Fed. Cir. 2009) (quoting *CytoLogix Corp. v. Ventana Med. Sys., Inc.*, 424 F.3d 1168, 1172–73 (Fed. Cir. 2005)) (agreeing that it was improper for Boston Scientific “[i]n effect … to argue claim construction to the jury”). Indeed, it is reversible error for a district court to leave “the jury free to consider … arguments” that go to the proper construction of a patent claim. *O2 Micro*, 521 F.3d at 1362. A court simply cannot “delegat[e] to the jury the task of determining claim scope.” *Silver Spring Networks*, 2016 WL 766661, at \*3. Accordingly, the district court committed reversible error in allowing Prism to present a different claim construction to the jury.

At the *Daubert* stage, the district court allowed Prism to present its theory to the jury by concluding that the issue was “a question of fact,” namely the level of “sufficient control.” Appx94. The district court was wrong. According to Prism’s theory, the level of sufficiency is not a question about the level of control that Sprint has or the backhaul providers have over their backhauls; it is about the level of control required by the patented claims—whether they require no “single” controlling organization. As the district court initially framed the dispute, the parties’ argument was about whether the district court’s *Markman* order should govern or whether “Minor’s interpretation” is appropriate. Appx91. Indeed, as illustrated by the court, the issue presented to the court was whether the term “single” should be inserted into the claim construction to require “a public network with no *single* controlling organization,” or whether the initial construction of “no controlling organization” should remain. *Id.* Accordingly, the dispute was about the scope of the claims.

As this Court has explained, the “scope of the asserted claims is a question of law.” *O2 Micro*, 521 F.3d at 1361. “When the parties raise an actual dispute regarding the proper scope of these claims, the court,

not the jury, must resolve that dispute.” *Id.* at 1360. Here, the district court allowed Prism to present a different scope for the asserted claims, one that required “no single controlling organization,” rather than “no controlling organization.” This altered the type of network that qualified as “untrusted” for purposes of the asserted claims. Under this Court’s precedent, that was error. The court, not the jury, should resolve issues regarding the scope of the asserted claims. The district court erred.

**2. Prism compounded the court’s error by redefining the “path to access” requirement.**

Prism compounded the district court’s error by also arguing a different construction of the “path to access” requirement for an untrusted network. The district court held that an untrusted network is one where the “path to access the network” is “undefined.” Prism’s theory and case relied on a different construction—one in which the “path through” an untrusted network is undefined.

The theory that Prism presented to the jury was not that Sprint’s “path to access” an untrusted network was undefined. It was that “the path *through* the network to access” the data center changes as a user travels from one cell tower location to another. Appx26950–51 (Tr.

487:24–488:25); *see also* Appx29650–53 (Tr. 487:16–490:5); Appx26894 (Tr. 431:9–25). In other words, as a user travels around town or from town to town, the cellular tower will change and so “the path through the network to access” the data center “changes as you travel.” Appx26950–51 (Tr. 487:24–488:25). This is nothing short of an unabashed re-write of the district court’s claim construction.

The district court adopted the specification’s explicit definition of “untrusted,” which makes clear that “the path *to* access the network [is] undefined” in the invention. Appx156 (’345 patent 3:49–52) (emphasis added). The court’s and specification’s definition does not address how information moves through the network to reach the server, which is the data center under Prism’s theory. It says only that the path to access the network, which according to Prism is the Ethernet backhaul, must be undefined. Prism’s theory fundamentally alters the scope of the claims. The definition of “Internet Protocol network,” according to Prism, no longer looks at how data accesses the network, but how it ultimately accesses the server. Such a fundamental rewrite of the claims’ scope was an issue for the court, not the jury. *Silver Spring*

*Networks*, 2016 WL 766661, at \*3 (agreeing that it is improper to “delegat[e] to the jury the task of determining claim scope”).

The district court erred in allowing Prism to argue a different claim construction of the “Internet Protocol network” limitation to the jury. That error at a minimum requires a new trial, but given the undisputed evidence, should warrant reversal. *Id.* at \*5 & n.3.

**II. ADMISSION OF THE SETTLEMENT AGREEMENT BETWEEN PRISM AND AT&T VIOLATED FEDERAL RULES OF EVIDENCE 403 AND 408 AND REQUIRES A NEW TRIAL.**

The district court also erred in allowing Prism to introduce testimony and evidence of AT&T’s Settlement, which was agreed to [REDACTED] [REDACTED] The district court denied Sprint’s motion in limine to exclude this evidence with no discussion whatsoever of Sprint’s arguments or this Court’s controlling authority, stating simply that Sprint’s motion was “Denied.” Under this Court’s precedents, however, such settlement agreements are presumptively inadmissible and must be excluded except in specific limited circumstances not met by the AT&T Settlement. The district court’s admission of this evidence constituted legal error for two separate reasons: 1) it violated this Court’s precedents on the admission

of such agreements under Rule 403; and 2) Prism used the evidence to establish the validity and amount of its claim against Sprint in violation of Rule 408. Each error independently requires a new trial.

**A. Admission of the AT&T Settlement Violated Federal Rule of Evidence 403.**

This Court’s precedents establish that settlement licenses are presumptively inadmissible to prove a reasonable royalty for related patents. As this Court has stated, such settlement agreements must be excluded except in “certain limited circumstances.” *LaserDynamics*, 694 F.3d at 77. Because the AT&T Settlement is “well outside the limited scope of circumstances under which” this Court will deem settlement agreements “admissible and probative,” *id.* at 78, the district court abused its discretion in admitting evidence of the AT&T Settlement. A new trial is warranted.

In *LaserDynamics*, this Court recognized that “the propriety of using prior settlement agreements to prove the amount of a reasonable royalty” is “questionable.” *Id.* at 77. In reaching this conclusion, the Court explained that Rule 403 provides for exclusion of evidence when the danger of undue prejudice outweighs its probative value and that Rule 408 “specifically prohibits” use of settlement agreements to prove

damages. *Id.* This Court also relied on the Supreme Court’s decision in *Rude v. Westcott*, which explained that “a payment of any sum in settlement of a claim for an alleged infringement cannot be taken as a standard to measure the value of the improvements patented, in determining the damages sustained by the owners of the patent in other cases of infringement.” 130 U.S. 152, 164 (1889). The default rule is, therefore, that settlement agreements are inadmissible.

This presumptive inadmissibility of settlement agreements accords with the *Georgia-Pacific Corp. v. U.S. Plywood Corp.*<sup>6</sup> factors—which this Court has held “properly tie the reasonable royalty calculation to the facts of the hypothetical negotiation at issue,” *Uniloc USA, Inc. v. Microsoft Corp.*, 632 F.3d 1292, 1317 (Fed. Cir. 2011). Those factors rest on the premise that “a voluntary agreement will be reached between a willing licensor and a willing licensee, with validity and infringement of the patent not being disputed.” *LaserDynamics*, 694 F.3d at 77. As a result, “license fees that are tainted by the coercive

---

<sup>6</sup> 318 F. Supp. 1116 (S.D.N.Y. 1970) modified *sub nom. Georgia-Pac. Corp. v. U.S. Plywood-Champion Papers, Inc.*, 446 F.2d 295 (2d Cir. 1971).

environment of patent litigation are *unsuitable* to prove a reasonable royalty.” *Id.* (emphasis added).

This Court has recognized only a very narrow exception to the general rule of inadmissibility of settlement agreements. In *ResQNet.com, Inc.*, this Court permitted reliance on a “lone settlement agreement [that stood] apart from all other licenses in the record as being uniquely relevant and probative.” *LaserDynamics*, 694 F.3d at 78 (citing *ResQNet.com, Inc. v. Lansa, Inc.*, 594 F.3d 860, 870–72 (Fed. Cir. 2010)). The *LaserDynamics* Court made clear that such circumstances are the rare exception to the “longstanding disapproval of relying on settlement agreements to establish reasonable royalty damages.” *Id.* at 77. Absent such unique limited circumstances, admitting evidence of a settlement agreement to establish a reasonable royalty is reversible error. *Id.*

Indeed, the Court’s decision in *LaserDynamics* resolves this case. There, this Court held that the district court abused its discretion in admitting a settlement agreement that was “executed shortly before a trial,” in an amount that was “six times larger than the next highest amount paid for a license to the patent-in-suit, and ostensibly reflects

not the value of the claimed invention but the strong desire to avoid further litigation under the circumstances.” *Id.* at 78. In addition, the challenged settlement was “entered into a full three years after the hypothetical negotiation date,” and was “in many ways not relevant to the hypothetical negotiation analysis.” *Id.* And there were multiple other licenses for the patent-in-suit that were “not settlements of active litigation” and were “far more reliable indicators of what willing parties would agree to in a hypothetical negotiation.” *Id.* The settlement agreement in *LaserDynamics* thus stood in “stark contrast” to the “limited scope of circumstances” in which such agreements are admissible. *Id.*

The same is true here. The AT&T Settlement Agreement was entered into not merely under the threat of litigation but at the height of trial, [REDACTED]

[REDACTED] Appx27148 (Tr. 685:6–10). [REDACTED]  
[REDACTED]

[REDACTED] The agreement was executed two and a half years after the hypothetical negotiation date. Appx27148, 27218 (Tr. 685:1–3,

755:15–18). And the agreement was less reliable by far than Prism’s other licenses: [REDACTED]

[REDACTED] See

*Lucent Techs., Inc. v. Gateway Inc.*, 580 F.3d 1301, 1328 (Fed. Cir. 2009) (rejecting reliance on a settlement agreement that “appear[ed] to govern [the plaintiff’s] entire patent portfolio” and thus “is directed to a vastly different situation than the hypothetical licensing scenario of the present case involving only one patent”). As in *LaserDynamics*, the “probative value of the [AT&T] settlement agreement is dubious in that it has very little relation to demonstrated economic demand for the patented technology.” *Id.* at 78. The district court failed to address, or indeed even mention, *LaserDynamics* or any of Sprint’s arguments

demonstrating the court's legal error in admitting the settlement agreement. Appx4–5.

The undue prejudice to Sprint from the admission of this evidence is palpable. As shown above, Prism's case on the merits was built on sophistry, arguing a different claim construction to the jury than the one adopted by the court. To disguise that fundamental flaw, Prism made the AT&T Settlement a cornerstone of its case, highlighting the settlement to the jury throughout the trial. Prism repeatedly equated Sprint with AT&T and used the AT&T Settlement Agreement to suggest that Sprint was liable for infringement and should be required to pay even more than [REDACTED] as a penalty for going to trial. *Supra* 22–26. Prism's counsel drove home this refrain in closing arguments, underscoring that AT&T “got a huge discount” because “[t]hey didn't make me stand here in front of a jury like you guys and do this.” Appx27933–34 (Tr. 1470:25–1471:2). The jury's damage award against Sprint strongly demonstrates the undue prejudicial effect of the AT&T Settlement: the jury awarded Prism \$30 million, which amounts to [REDACTED]

[REDACTED] Because the undue prejudice of allowing Prism to

introduce this evidence vastly outweighs its probative value, its admission violated Federal Rule of Evidence 403.

The AT&T Settlement Agreement is “well outside the limited scope of circumstances” in which a settlement agreement may be considered “admissible and probative.” *LaserDynamics*, 694 F.3d at 78. The district court’s abuse of discretion in admitting the settlement requires a new trial.

#### **B. Admission of the AT&T Settlement Violated Federal Rule of Evidence 408.**

The district court’s admission of the AT&T Settlement Agreement requires a new trial for the additional, independent reason that admitting the settlement violated Rule 408, and it did so twice-over. This Court has repeatedly recognized that under Rule 408, evidence of settlement agreements is “not *admissible*—on behalf of any party—either to prove or disprove the validity or amount of a disputed claim or to impeach by a prior inconsistent statement or a contradiction.” *In re MSTG, Inc.*, 675 F.3d 1337, 1343–44 (Fed. Cir. 2012). The rule “specifically prohibits the admission of settlement offers and negotiations offered to prove the amount of damages owed on a claim.” *LaserDynamics*, 694 F.3d at 77. Although this Court has “not yet

decided the extent to which evidence of settlement negotiations would be admissible under Rule 408,” *MSTG*, 675 F.3d at 1346, n.4, it is clear that under Rule 408, settlement evidence is admissible “only for purposes *other than proving liability or the amount of a claim.*” *MSTG*, 675 F.3d at 1344 (emphasis added). However, that is precisely why Prism introduced this evidence. It used the AT&T Settlement to prove *both* the amount of the claim and Sprint’s liability. Either violation requires a new trial.

Rule 408 provides that evidence of “furnishing, promising, or offering—or accepting, promising to accept, or offering to accept—a valuable consideration in compromising or attempting to compromise the claim” is “not admissible—on behalf of any party—either to prove or disprove the validity or amount of a disputed claim.” Fed. Rule Evid. 408(a)(1). This rule plainly applies to Prism’s settlement agreement with AT&T. As this Court has explained, “[t]he rule is clear by its text and history that it covers not only settlements and negotiations between the parties to the lawsuit, but also settlements and negotiations involving a third party.” *MSTG*, 675 F.3d at 1347. This view is supported by the Rule’s advisory committee notes, which explain

that the rule applies to “completed compromises” such as “when a party to the present litigation has compromised with a third person,” Fed. R. Evid. 408 advisory committee’s note (1972 Proposed Rules), and that it “excludes compromise evidence even when a party seeks to admit its own settlement offer or statements made in settlement negotiations,” *id.* (2006 Amendment). The district court therefore erred in admitting evidence of the AT&T Settlement Agreement to prove either liability or damages.

As demonstrated above, Prism introduced the AT&T Settlement Agreement at trial for the express purpose of establishing the amount of damages. Prism’s expert relied on the AT&T Settlement Amount in reaching his conclusion regarding a reasonable royalty. And Prism repeatedly emphasized that its claim against Sprint was worth as much as—indeed more than—[REDACTED] *Supra* 22–26.

This use of the AT&T Settlement to establish the amount of Prism’s claim violated the plain prohibition of Rule 408 and requires a new trial. *See Pioneer Hi-Bred Int’l, Inc. v. Ottawa Plant Food, Inc.*, 219 F.R.D. 135, 144 (N.D. Iowa 2003) (settlement agreements with other defendants cannot be admitted to show the amount of the claim against

the remaining defendant); *cf. Kennon v. Slipstreamer, Inc.*, 794 F.2d 1067, 1070 (5th Cir. 1986) (“Disclosing the amount of settlement had no proper purpose in the circumstances of this case and therefore it violated Rule 408.”); *Playboy Enterprises, Inc. v. Chuckleberry Pub., Inc.*, 687 F.2d 563, 569 (2d Cir. 1982).

The district court’s and Prism’s violation of Rule 408 did not stop there. Prism repeatedly invoked the AT&T Settlement not merely to establish the amount of its claim, but also to establish Sprint’s liability for infringement. Rule 408 plainly prohibits admission of settlement evidence to prove *the validity* of a claim. *Cf. McHann v. Firestone Tire & Rubber Co.*, 713 F.2d 161, 166 (5th Cir. 1983) (settlement evidence inadmissible because it could lead the jury to base its decision on the perception that payment of a substantial sum means that the paying party is at fault). Prism’s story to the jury was that AT&T and Sprint were essentially equivalent and engaged in the same activity with regard to the asserted claims, that AT&T settled with Prism [REDACTED]

[REDACTED] and that Sprint therefore was liable just like AT&T, but should be punished for not settling. Duman testified that AT&T and Sprint have “a lot of similarities,” that Prism’s litigation

with AT&T was “on the same patents for essentially the – the same activity,” [REDACTED]

[REDACTED]

[REDACTED] Appx27145, 27146, 27148, 27155–56

(Tr. 682:23–25, 683:2–6, 685:6–10, 692:25–693:5). Prism’s expert and Prism’s counsel further hammered on this point: AT&T’s Settlement establishes that AT&T infringed, Sprint is the same as AT&T, so Sprint also infringes. *Supra* 22–26.

The district court abused its discretion in allowing Prism to introduce the AT&T Settlement to establish the validity of its claim. This separate violation of Rule 408 independently requires a new trial.

### **III. THE DISTRICT COURT APPLIED THE WRONG STANDARD IN REVIEWING SPRINT’S POST-TRIAL MOTIONS AND UTTERLY FAILED TO CONSIDER MULTIPLE GROUNDS FOR RELIEF.**

Although the grounds above alone warrant reversal, the Court should, at a bare minimum, reverse and remand because the district court applied the wrong legal standard and utterly failed to consider the multiple legal errors identified by Sprint’s motion for a new trial.

Sprint’s new trial motion challenged seven legal errors by the district

court, each of which independently merited a new trial. Appx23876 (Doc. 487). Sprint also argued that a new trial was required because, absent certain improperly admitted evidence, the jury's verdict was against the weight of the evidence. *Id.* The district court failed to consider any of Sprint's legal challenges, addressing only the weight of the evidence.

The sum total of the district court's analysis of Sprint's eight-point motion for a new trial was:

A motion for new trial is governed by Federal Rule of Civil Procedure 59. The standard for granting a new trial is whether the verdict is against "the great weight of the evidence." *Butler v. French*, 83 F.3d 942, 944 (8th Cir. 1996). In evaluating a motion for a new trial pursuant to Rule 59(a), the "key question is whether a new trial should have been granted to avoid a miscarriage of justice." *McKnight By & Through Ludwig v. Johnson Controls, Inc.*, 36 F.3d 1396, 1400 (8th Cir. 1994).

After reviewing [the] facts, evidence, and the relevant law, the Court cannot say that the jury's verdict was against the great weight of the evidence. Therefore, the Court will deny the defendant's motion for new trial.

Appx4–5. In denying Sprint's motion solely on the basis that "the Court cannot say that the jury's verdict was against the great weight of the evidence," Appx5, the court either utterly ignored the seven legal errors

that resulted in a miscarriage of justice in this case or improperly treated Sprint's legal challenges as weight of the evidence challenges. This was error.

As Sprint explained to the district court, “[a] new trial is appropriate” when a miscarriage of justice arises from any one of three independent grounds: (1) “a verdict [is] against the weight of the evidence,” (2) there is “an excessive damage award,” (3) “or” there are “*legal errors at trial.*” Appx23889 (Doc. 487 at 5) (emphases added) (quoting *Gray*, 86 F.3d at 1480). Sprint further explained that the court may grant a new trial “where improper evidentiary rulings ‘had a substantial influence on the jury’s verdict,’” and “the admission of evidence was ‘so prejudicial that a new trial would likely produce a different result.’” Appx23889 (quoting *Littleton v. McNeely*, 562 F.3d 880, 888 (8th Cir. 2009), and *Harrison v. Purdy Bros. Trucking Co.*, 312 F.3d 346, 351 (8th Cir. 2002)). The district court ignored controlling Eighth Circuit authority.

Because the district court failed to recognize that a new trial may be warranted based on “legal errors at trial,” *Gray*, 86 F.3d at 1480–81 , and to address any of the legal errors Sprint raised in its new trial

motion, this Court, at a minimum, should reverse the district court’s denial of a new trial.

#### **IV. THE DISTRICT COURT ERRED IN ADMITTING PRISM’S COST-SAVINGS DAMAGES THEORY, WHICH FAILS TO REFLECT THE FOOTPRINT OF THE INVENTION.**

Even if the Court does not remand for a new trial on the merits, it should do so for the award of damages in this case. A basic tenet of this Court’s precedents is that a reasonable royalty must be based on the footprint of the invention to ensure that damages compensate only for infringement of the patented features. In violation of this fundamental principle, Prism’s theory of damages was based not on the invention but rather on background technology that Prism concedes it did not invent. The district court’s error in admitting this damages theory warrants a new trial.

##### **A. A Reasonable Royalty Must Be Closely Tied To The Footprint Of The Invention.**

This Court has instructed that “[a]t all times, the damages inquiry must concentrate on compensation for the economic harm caused by infringement of the claimed invention,” and therefore “the trial court must carefully tie proof of damages to the claimed invention’s footprint in the market place.” *ResQNet.com*, 594 F.3d at 869 (citing *Aro Mfg. Co.*

v. Convertible Top Replacement Co., 377 U.S. 476, 507 (1964) (“[T]he present statutory rule is that only ‘damages’ may be recovered.”)). Indeed, “[no] matter what the form of the royalty, a patentee must take care to seek only those damages attributable to the infringing features.” *VirnetX, Inc. v. Cisco Sys., Inc.*, 767 F.3d 1308, 1326 (Fed. Cir. 2014). To avoid overvaluing a patent’s contribution, the Supreme Court has mandated that “the patentee … must in every case give evidence tending to separate or apportion the defendant’s profits and the patentee’s damages between the patented feature and the unpatented features, and such evidence must be reliable and tangible, and not conjectural or speculative.” See *Uniloc USA, Inc.*, 632 F.3d at 1318 (citing *Garretson v. Clark*, 111 U.S. 120, 121 (1884)).

This requirement to tailor damages to the claimed invention reflects the statutory limitation entitling a patentee to “damages adequate to compensate for the infringement.” 35 U.S.C. § 284 (emphasis added). “Any evidence unrelated to the claimed invention does not support compensation for infringement but punishes beyond the reach of the statute.” *ResQNet.com*, 594 F.3d at 869; see *Lucent*, 580 F.3d at 1333 (granting new trial where royalty analysis did not properly

account for profit attributable to patented feature “compared to non-patented elements and other features”). A damages model that fails to reflect the footprint of the invention is therefore inadmissible.

#### **B. Prism’s Damages Expert Failed to Tie His Model to the Invention.**

Prism’s damages model violated the statutory command and this Court’s precedents by basing the cost-savings analysis not on the asserted invention—*i.e.*, authentication of users to allow access to secure computer resources—but rather on the Ethernet backhaul, which Prism concedes it did not invent.<sup>8</sup> As Prism itself described the invention: “You have a development that was done to allow devices to get authenticated to get access ... to something and the motivating factor was to do it on the open Internet. [T]here’s no dispute about that. But Prism didn’t invent ... a new Internet or a new private network. They invented technology, systems and methods ... to accomplish a particular result.” Appx9707. Prism’s invention is thus not the backhaul or a new untrusted network; it is the authentication of users to allow access to protected computer resources over that network.

---

<sup>8</sup> Prism’s sole focus on the Ethernet backhaul to supports its damages theory shows that any discussion of femtocells, picocells, or roaming is a red herring.

The patents themselves prove that the invention is not the untrusted network, which is included in the description of the prior art. Appx155 ('345 patent 1:29–31); Appx223 ('155 patent 1:29–31). Instead the “present invention generally relates to security systems *for use with* computer networks.” Appx155 ('345 patent 1:15–19); Appx223 ('155 patent 1:15–19) (emphasis added). It “discloses a system for securing and tracking usage of transaction services or computer resources.” Appx155 ('345 patent 1:60–61); Appx223 ('155 patent 1:60–61). Prism’s lead inventor, Richard Gregg, characterized his “aha moment” when he knew he had an invention as “the addition of the hardware component, the access key or hardware key, the use of a hardware component in the invention,” not the discovery of the Internet or an untrusted network. Appx24802–03; *see also* Appx24811–12 (Sandeep Giri: “writing a system at the time that used a hardware key was different from the status quo solution in the market at the time.”). Prism’s invention was thus the authentication system, specifically one using a hardware key, not a backhaul, network, Ethernet, or Internet.

Yet, rather than identifying cost savings based on a noninfringing alternative to the *invention*, Prism’s expert improperly based his cost-

savings model on the non-inventive Ethernet backhaul. Specifically, although the patents make clear that authentication systems to restrict access to protected resources over untrusted networks were known, Appx155 ('345 patent 1:34–39), Malackowski testified that without the patented invention, Sprint would have to build or purchase its own backhauls rather than lease backhaul services from AAVs. *See, e.g.*, Appx27227(Tr. 764:3–8). He then calculated the cost savings (or, more accurately, he *purported* to do so, *see infra* 67–69) to Sprint from not having to build or purchase its own backhaul. Malackowski's damages model is therefore simply untethered from the invention—*i.e.*, Prism's authentication system—and instead is based on “evidence unrelated to the claimed invention”—*i.e.*, the Ethernet backhaul. Basing damages on such unrelated evidence “punishes beyond the reach of the statute.”

*ResQNet*, 594 F.3d at 869.

By calculating damages based on the Ethernet backhaul, Prism seeks payment for something it did not invent. This Court has refused to allow such overreaching. In *Riles v. Shell Expl. & Prod. Co.*, 298 F.3d 1302 (Fed. Cir. 2002), the patentee of a method for installing drilling platforms using temporary pilings rather than mud mats sought as

damages the entire cost of the defendant’s drilling platform. This Court rejected such a damages model, noting that “the market would pay [the patentee] only for his product a method of anchoring offshore oil rigs without mud mats,” and that the damages expert did “not associate his proposed royalty with the value of the patented method at all, but with the unrelated cost of the entire Spirit platform, which includes much more than the cost of anchoring without mud mats.” 298 F.3d at 1312. Because the damages model did “not account for the actual losses due to infringement of the patented method,” it could not support the jury’s verdict. *Id.*; see also *Monsanto Co. v. McFarling*, 488 F.3d 973, 980–81 (Fed. Cir. 2007) (approving cost savings analysis based on costs of using the prior art versus using the patented invention).

Likewise here, Prism’s damages model does not associate the proposed royalty with the patented invention of user authentication and thus does not account for the actual losses due to infringement of the footprint of the invention. Instead, it impermissibly accounts for the unrelated cost of the Ethernet backhaul with which the invention can be used, a cost “which includes much more than the cost of [authenticating users to allow access to secured resources.]” *Id.* Prism

did not invent the backhaul, and the district court erred in admitting a damages model based on the backhaul rather than the footprint of the invention.

**C. Even If It Were Permissible to Measure Damages Based on the Non-Patented Backhaul, Prism's Model Nonetheless Impermissibly Departs from the Footprint of the Invention and Is Otherwise Unreliable.**

Reversal of the award of damages is also warranted for a separate reason. In purporting to calculate cost savings based on the cost of building or purchasing a new backhaul, Malackowski improperly equated the actual cost of leasing a backhaul with the hypothetical cost of building or purchasing backhauls, further detaching the damages model from the footprint of the invention. In calculating his royalty base, Malackowski relied on Prism's technical expert's vague and baseless speculation that building a backhaul would cost Sprint "two to three times ... and ... potentially ... more than five times" as much as Sprint spends on leasing a backhaul. Appx27231 (Tr. 768). Malackowski thus calculated damages based on Sprint's actual *expenditures*—which he conceded [REDACTED]—rather than its alleged cost *savings*.

This approach further unmoored the damages model from the footprint of the invention. The cost to lease backhaul networks fluctuates depending on a number of factors, some technological and some business-related, that have nothing whatsoever to do with the claimed invention of user authentication. Appx27284–85 (Tr. 821:25–822:4). For example, vendors may charge a premium for a shorter repair time in the event data transmission becomes unavailable or may offer discounts to high volume users. Appx27285–86 (Tr. 822–823); Appx17668. Factors like the volume of data a company sends over a backhaul or the speed with which the vendor repairs data transmission interruptions bear no relation to Prism’s user authentication invention. Yet, as Malackowski unreservedly conceded, under his damages model, every dollar Sprint spends to lease a backhaul increases the royalty base proportionally. Appx27287–89 (Tr. 824:1–4; 824:7–14; 824:19–825:6; 825:21–826:7). As a result, even under Prism’s view of the footprint of the invention, Malackowski’s damages model fails to carefully tie the reasonable royalty to the patent.

In any event, Malackowski’s opinion based on Sprint’s actual expenditures to lease backhaul services is unreliable on its own terms.

As noted above, Malackowski relied on the statement by Minor, Prism's technical expert, that building or purchasing a backhaul would cost Sprint "two to three times ... and ... potentially ... more than five times" as much as Sprint spends on leasing a backhaul. Appx27231 (Tr. 768). But Minor lacked any factual basis for this assertion or any expertise in valuation and accounting. Minor admitted that he had no way to calculate the actual cost savings over building a backhaul, that he "generalize[d] the savings," that he did not rely on any actual Sprint backhaul expense data, that he prepared no mathematical computations of the costs, and that he did not consider actual mileage to cell sites, actual fiber costs, or circuit costs. Appx26962, 26993, 27065–66 (Tr. 499, 530, 602–03). Malackowski's opinion based on Minor's speculative and baseless guess as to the costs of building a backhaul system should have been excluded as unreliable. "Expert testimony relying on the opinions of others should, of course, be rejected if the testifying expert's opinion is too speculative, or the underlying basis is faulty." *Walker v. Soo Line R. Co.*, 208 F.3d 581, 588 (7th Cir. 2000) (citations omitted). Because the district court erred in admitting

this damages model, this Court should, at a minimum, order a new trial on damages.

## CONCLUSION

For the foregoing reasons, the Court should reverse the judgment, or, at minimum, reverse and remand for a new trial.

Respectfully submitted,

Dated: March 31, 2016

/s/ Carter G. Phillips

CARTER G. PHILLIPS  
RYAN C. MORRIS  
JENNIFER J. CLARK  
SIDLEY AUSTIN LLP  
1501 K Street, N.W.  
Washington, D.C. 20005  
Telephone: (202) 736-8000  
Facsimile: (202) 736-8711

MICHAEL J. BETTINGER  
IRENE YANG  
SIDLEY AUSTIN LLP  
555 California Street, Suite  
2000  
San Francisco, California  
94104  
Telephone: (415) 772-1200  
Facsimile: (415) 772-7400

*Counsel for Sprint Spectrum L.P.*

## **CERTIFICATE OF COMPLIANCE**

This brief complies with the type-volume limitations of Federal Rule of Appellate Procedure 32(a)(7)(B) and the Rules of this Court, because it contains 13,580 words (as determined by the Microsoft Word 2010 word-processing system used to prepare the brief), excluding the parts of the brief exempted by Federal Rule of Appellate Procedure 32(a)(7)(B)(iii).

This brief also complies with the typeface requirements of Federal Rule of Appellate Procedure 32(a)(5) and the type-style requirements of Federal Rule of Appellate Procedure 32(a)(6) because it has been prepared in a proportionally spaced typeface using the Microsoft Word 2010 word-processing system in 14-point Century Schoolbook font.

/s/ Ryan C. Morris

## **CERTIFICATE OF SERVICE**

I hereby certify that on this 31st day of March, 2016, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Federal Circuit through the Court's CM/ECF system.

Participants in the case who are registered CM/ECF users will be served by the appellate CM/ECF system.

/s/ Ryan C. Morris  
\_\_\_\_\_  
Ryan C. Morris

# **ADDENDUM**

## ADDENDUM TABLE OF CONTENTS

Judgment .....	Appx1
Memorandum Opinion on Defendant's Post-Trial Motions.....	Appx2
Order and Judgment on Defendant's Post-Trial Motions .....	Appx7
Memorandum Opinion on Plaintiff's Motion for Prejudgment and Postjudgment Interest and for an Accounting and Ongoing Royalties.....	Appx8
Order and Judgment on Plaintiff's Motions for Prejudgment and Postjudgment Interest and for an Accounting and Ongoing Royalties.....	Appx14
Claim Construction Ruling .....	Appx16
Ruling on Defendant's Common Daubert Motion to Exclude the Opinions and Testimony of Plaintiff's Expert John Minor.....	Appx84
Ruling on Defendant's Second Common Daubert Motion to Exclude the Opinions and Testimony of Plaintiff's Damages Expert James E. Malackowski.....	Appx95
Ruling on Cross Motions in Limine .....	Appx102
Trial Exhibit 1 – U.S. Patent No. 8,127,345 .....	Appx108
Trial Exhibit 2 – U.S. Patent No. 8,387,155 .....	Appx175

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC,	)	
	)	8:12CV123
Plaintiff,	)	
	)	JUDGMENT
v.	)	
	)	
SPRINT SPECTRUM L.P., D/B/A	)	
SPRINT PCS,	)	
Defendant.	)	

This action came before the Court for trial by jury. The issues have been tried and the jury has rendered its verdict.

**IT IS ORDERED AND ADJUDGED** that judgment is entered in favor of the Plaintiff, Prism Technologies, LLC, and against Defendant, Sprint Spectrum L.P., d/b/a Sprint PCS, in the amount of \$30,000,000.00 together with the Plaintiff's costs herein.

Dated this 24th day of June 2015.

DENISE M. LUCKS  
Clerk of Court

By : s/Mary Roundtree  
Deputy Clerk

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC,	)	
	)	
Plaintiff,	)	8:12CV123
	)	
v.	)	
	)	
SPRINT SPECTRUM L.P.,	)	MEMORANDUM OPINION
d/b/a SPRINT PCS,	)	
	)	
Defendant.	)	
	)	

---

This matter is before the Court on defendant, Sprint Spectrum L.P.'s ("Sprint"), post trial motions. Presently pending in this case are defendant's renewed motion for judgment as a matter of law (Filing No. 490), motion for new trial (Filing No. 486), and motion for relief filed pursuant to Federal Rule of Civil Procedure 60(b), or in the alternative, motion for leave to supplement the motion for new trial (Filing No. 576). All motions have been fully briefed and are ready for disposition. After reviewing the motions, briefs, indices of evidence, and applicable law, the Court finds as follows.

**I. Renewed Motion for Judgment as a Matter of Law**

In patent cases, a motion for judgment as a matter of law pursuant to Rule 50(b) is reviewed under the law of the regional circuit. *Synthes USA, LLC v. Spinal Kinetics, Inc.*, 734

F.3d 1332, 1340 (Fed. Cir. 2013). When considering a motion for judgment as a matter of law, a court "must determine whether or not the evidence was sufficient to create an issue of fact for the jury." *Lane v. Chowning*, 610 F.2d 1385, 1388 (8th Cir. 1979). The Court will grant a motion for judgment as a matter of law "when all the evidence points one way and is susceptible of no reasonable inferences sustaining the position of the nonmoving party." *Ehrhardt v. Penn. Mut. Life Ins. Co.*, 21 F.3d 266, 269 (8th Cir. 1994). In considering the motion, the Court views the record in the light most favorable to the prevailing party. *Wash Solutions, Inc. v. PDQ Mfg., Inc.*, 395 F.3d 888, 892 (8th Cir. 2005). The Court must also assume that all conflicts in the evidence were resolved in favor of the prevailing party, and the Court must assume as proved all facts that the prevailing party's evidence tended to prove. *E.E.O.C. v. Kohler Co.*, 335 F.3d 766, 772 (8th Cir. 2003). The motion should be denied unless the Court concludes that no reasonable juror could have returned a verdict for the nonmoving party. *Billingsley v. City of Omaha*, 277 F.3d 990, 995 (8th Cir. 2002).

Sprint alleges that Prism failed to offer legally sufficient evidence at trial that Sprint infringes the asserted patents. Sprint's renewed motion for judgment as a matter of law focuses on Prism's theory that third-party AAV backhaul providers

satisfy the "Internet Protocol Network" limitations. Sprint argues that it does not control the third-party AAV backhaul providers or its customers who operate the client computer device; therefore, it does not infringe the asserted claims.

Reviewing the record in the light most favorable to the prevailing party, the Court finds that Prism presented sufficient evidence at trial that a reasonable juror could find that Sprint infringed the asserted patents. A reasonable juror could determine, based on the evidence presented at trial, that Sprint alone performed the steps to control access to protected computer resources provided over an untrusted internet protocol network. In addition, the claims do not require Prism to show that Sprint controls its customers to prove infringement. As a result, the Court will deny Sprint's renewed motion for judgment as a matter of law.

## **II. Motion for New Trial**

A motion for new trial is governed by Federal Rule of Civil Procedure 59. The standard for granting a new trial is whether the verdict is against "the great weight of the evidence." *Butler v. French*, 83 F.3d 942, 944 (8th Cir. 1996). In evaluating a motion for a new trial pursuant to Rule 59(a), the "key question is whether a new trial should have been granted

to avoid a miscarriage of justice." *McKnight By & Through Ludwig v. Johnson Controls, Inc.*, 36 F.3d 1396, 1400 (8th Cir. 1994).

After reviewing the facts, evidence, and the relevant law, the Court cannot say that the jury's verdict was against the great weight of the evidence. Therefore, the Court will deny the defendant's motion for new trial.

**III. Motion for Relief under Federal Rule of Civil Procedure 60(b)**

Under Federal Rule of Civil Procedure 60(b), "a court may relieve a party or its legal representative from a final judgment, order, or proceeding" for various reasons. Sprint moves this Court to set aside the judgment pursuant to Rule 60(b) (5) and (6), which authorizes a court to relieve a party when "the judgment has been satisfied, released, or discharged; it is based on an earlier judgment that has been reversed or vacated; or applying it prospectively is no longer equitable; or any other reason that justifies relief." "Rule 60(b) 'provides for extraordinary relief which may be granted only upon an adequate showing of exceptional circumstances.'" *Atkinson v. Prudential Property Co., Inc.*, 43 F.3d 367, 371 (8th Cir. 1994) (quoting *United States v. Young*, 806 F.2d 805, 806 (8th Cir. 1986) (per curiam)). Relief may be granted "only where exceptional circumstances have denied the moving party a full and

fair opportunity to litigate his claim and have prevented the moving party from receiving adequate redress." *Harley v. Zoesch*, 413 F.3d 866, 871 (8th Cir. 2005) (citing *Atkinson*, 43 F.3d at 373)).

Sprint alleges that the Court altered the claim construction for "authentication server" when the Court answered a jury question in the T-Mobile trial (*See Prism Technologies LLC v. T-Mobile USA, Inc.*, 8:12CV124). The Court did not change the claim construction by answering the jury's question. In addition, Sprint did not present a non-infringement theory at trial regarding the authentication server. Sprint now wants to rely on an answer to a jury question from a trial with different systems and evidence. Sprint has failed to show an exceptional circumstance for which relief could be granted. As a result, the Court will deny Sprint's motion for relief from judgment under Rule 60(b), or in the alternative, motion for leave to supplement Sprint's motion for new trial.

A separate order will be entered in accordance with this memorandum opinion.

DATED this 9th day of December, 2015.

BY THE COURT:

/s/ Lyle E. Strom

---

LYLE E. STROM, Senior Judge  
United States District Court

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC, )  
                              )  
Plaintiff,                 )                           8:12CV123  
                              )  
v.                         )  
                              )  
SPRINT SPECTRUM L.P.,     )                           ORDER AND JUDGMENT  
d/b/a SPRINT PCS,         )  
                              )  
Defendant.                 )  
\_\_\_\_\_)

Pursuant to the memorandum opinion entered herein this date,

IT IS ORDERED:

- 1) Defendant's renewed motion for judgment as a matter of law (Filing No. 490) is denied.
- 2) Defendant's motion for new trial (Filing No. 486) is denied.
- 3) Defendant's motion for relief from judgment pursuant to Federal Rule of Civil Procedure 60(b), or in the alternative, motion for leave to supplement Sprint's motion for new trial, (Filing No. 576) is denied.

DATED this 9th day of December, 2015.

BY THE COURT:

/s/ Lyle E. Strom

---

LYLE E. STROM, Senior Judge  
United States District Court

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC,	)	
	)	
Plaintiff,	)	8:12CV123
	)	
v.	)	
	)	
SPRINT SPECTRUM L.P.,	)	MEMORANDUM OPINION
d/b/a SPRINT PCS,	)	
	)	
Defendant.	)	
	)	

---

This matter is before the Court on two related motions. The plaintiff, Prism Technologies, LLC ("Prism"), filed a motion for prejudgment and postjudgment interest to be paid by the defendant, Sprint Spectrum L.P., ("Sprint") (Filing No. 489). In addition, Prism filed a motion for an accounting and ongoing royalties (Filing No. 496). The two motions have been fully briefed and are ready for disposition. After reviewing the motions, briefs, indices of evidence, and the relevant law, the Court finds as follows.

**Background**

Prism brought suit against Sprint alleging patent infringement of U.S. Patent Nos. 8,127,345 and 8,387,155 (the "Asserted Patents"). A seven-day trial was held in June of 2015. On June 23, 2015, the jury returned a verdict in favor of Prism. The jury awarded Prism \$30 million in damages for Sprint's

infringement of the asserted patents. Prism moves this Court for prejudgment and postjudgment interest and for an accounting and ongoing royalties.

**Discussion**

**I. Motion for Prejudgment and Postjudgment Interest**

Prism moves this Court for an award of prejudgment and postjudgment interest. Prism suggests that prejudgment interest should be calculated using the prime rate compounded quarterly. Prism has submitted a calculation of prejudgment interest calculated by James E. Malackowski (Filing No. [493](#), Exhibit 5). Sprint alleges that the prejudgment interest, if awarded, should be calculated at the Treasury bond rate, compounded annually. Both parties agree that postjudgment interest is appropriate under 28 U.S.C. § 1961.

The Supreme Court has held that prejudgment interest should ordinarily be awarded in patent cases, but an award is not automatic. *General Motors Corp. v. Devex Corp.*, 461 U.S. 648, 103 S.Ct. 2058, 76 L.Ed.2d 211 (1983). "For example, it may be appropriate to limit prejudgment interest, or perhaps even deny it altogether, where the patent owner has been responsible for undue delay in prosecuting the lawsuit. There may be other circumstances in which it may be appropriate not to award prejudgment interest." *Bio-Rad Laboratories, Inc. v. Nicolet*

*Instrument Corp.*, 807 F.2d 964, 967 (Fed. Cir. 1986). Applying these standards, the Court finds that there are no circumstances precluding awarding prejudgment interest. However, the issue before the Court is what rate to apply to the awarded prejudgment interest.

Prism alleges that the prime rate is appropriate in calculating the prejudgment interest owed to Prism. However, Sprint claims that a prejudgment interest should be calculated at the Treasury bond rate. "Regarding the rate at which prejudgment interest is calculated, the district court has the discretion to determine whether to use the prime rate, the prime rate plus a percentage, the U.S. Treasury rate, state statutory rate, corporate bond rate, or whatever rate the court deems appropriate under the circumstances." *Century Wrecker Corp. v. E.R. Buske Mfg. Co., Inc.*, 913 F. Supp. 1256, 1280 (N.D. Iowa 1996). The Court finds that the prime rate at 3.25% would best compensates Prism for Sprint's infringement. As a result, the Court will grant Prism's motion for prejudgment interest to be calculated at the prime rate of 3.25% and compounded quarterly, totaling \$2,001,923.

Under 28 U.S.C. § 1961, "interest shall be allowed on any money judgment in a civil case recovered in a district court." Postjudgment interest "shall be calculated from the date

of the entry of the judgment, at a rate equal to the weekly average 1-year constant maturity Treasury yield . . . compounded annually." *Id.*

Both parties agree that Prism is entitled to postjudgment interest calculated using the Treasury bond rate pursuant to 28 U.S.C. § 1961. Prism alleges that postjudgment interest should be awarded inclusive of prejudgment interest and any award of ongoing royalties. The Court addresses Prism's motion for ongoing royalties below. The Court will grant the plaintiff's motion for postjudgment interest which shall be calculated using the "weekly average 1-year constant maturity Treasury yield . . . compounded annually" pursuant to 28 U.S.C. § 1961.

## **II. Motion for an Accounting and Ongoing Royalties**

Prism moves this Court for an accounting for Sprint's infringement after 2014 through the entry of judgment and to have a royalty set for ongoing infringement through the life of the Asserted Patents. Sprint opposes Prism's motion and alleges that both an accounting and ongoing royalties are improper. Sprint argues that the jury instructions were clear to provide Prism compensation for past, present, and ongoing infringement. Prism claims that an accounting and ongoing royalties would grant Prism with complete relief from the infringement.

Under 35 U.S.C. § 284, a prevailing patentee shall be awarded damages "adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer, together with interest and costs as fixed by the court." The district court has discretion to determine whether an ongoing royalty would be appropriate. The Court finds that the jury instructions were clear in providing Prism with complete relief from infringement. The jury was instructed that, "[T]he damages you award must be adequate to compensate Prism for the infringement . . . . Your damages award, if you reach this issue, should put Prism in approximately the same financial position that it would have been in had the infringement not occurred." (Filing No. [466](#) at 25). In addition, question 2 on the verdict form indicated that the jury would be awarding damages in the amount of a reasonable royalty. (See Filing No. [467](#)). The Court finds that an accounting and ongoing royalties would be inappropriate because the \$30 million jury verdict represents the jury's award of a reasonable royalty to compensate Prism for Sprint's past, present, and ongoing infringement. As a result, the Court will deny Prism's motion

for an accounting and ongoing royalties. A separate order will be entered in accordance with this memorandum opinion.

DATED this 18th day of December, 2015.

BY THE COURT:

/s/ Lyle E. Strom

---

LYLE E. STROM, Senior Judge  
United States District Court

IN THE UNITED STATES DISTRICT COURT  
FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC, )  
                               )  
Plaintiff,                 )                           8:12CV123  
                               )  
v.                         )  
                               )  
SPRINT SPECTRUM L.P.,     )                           ORDER AND JUDGMENT  
d/b/a SPRINT PCS,         )  
                               )  
Defendant.                 )  
\_\_\_\_\_  
)

Pursuant to the memorandum opinion entered herein this date,

IT IS ORDERED:

1) Prism's motion for prejudgment and postjudgment interest (Filing No. [489](#)) is granted.

Prejudgment interest shall be applied to the \$30 million dollar verdict at a prime rate of 3.25% and compounded quarterly resulting in the amount of \$2,001,923.

Postjudgment interest shall be calculated from the date of the entry of judgment using the weekly average 1-year constant maturity Treasury yield compounded annually pursuant to 28 U.S.C. § 1961.

Sprint shall pay Prism \$2,001,923 together with postjudgment interest from the date judgment, June 24, 2015, until satisfaction, in accordance with 28 U.S.C. § 1961.

2) Prism's motion for an accounting and ongoing royalties (Filing No. 496) is denied.

DATED this 18th day of December, 2015.

BY THE COURT:

/s/ Lyle E. Strom

---

LYLE E. STROM, Senior Judge  
United States District Court

IN THE UNITED STATES DISTRICT COURT FOR THE  
DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV122
	)	
v.	)	
	)	
AT&T MOBILITY, LLC,	)	MEMORANDUM AND ORDER
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV123
	)	
v.	)	
	)	
SPRINT SPECTRUM L.P.,	)	
d/b/a SPRINT PCS,	)	
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV124
	)	
v.	)	
	)	
T-MOBILE USA, INC.,	)	
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV125
	)	
v.	)	
	)	
UNITED STATES CELLULAR	)	
CORPORATION, d/b/a U.S.	)	
CELLULAR,	)	
	)	
Defendant.	)	
	)	

PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV126
	)	
v.	)	
	)	
CELLCO PARTNERSHIP d/b/a	)	
VERIZON WIRELESS,	)	
	)	
Defendant.	)	
	)	

---

This matter is before the Court for construction of patent claim terms in accordance with *Markman v. Westview Instruments, Inc.*, 517 U.S. 370 (1996). In these cases, plaintiff Prism Technologies LLC ("Prism") alleges infringement of three patents, U.S. Patent No. 7,290,288 ("'288 patent"), U.S. Patent No. 8,127,345 ("'345 patent"), and U.S. Patent No. 8,387,155 ("'155 patent") (collectively, the "asserted patents") by defendants AT&T Mobility LLC, Sprint Spectrum L.P., T-Mobile USA, Inc., United States Cellular Corporation d/b/a U.S. Cellular, and Cellco Partnership d/b/a Verizon Wireless. The parties have submitted proposed claim constructions, opening and responsive briefs, and corresponding indices of evidence, and the Court heard oral argument on July 2, 2013. After consideration of the briefs, evidence, oral argument, and relevant law, the Court rules as follows.

#### **I. Background and Procedural History.**

The '288 patent, entitled "METHOD AND SYSTEM FOR CONTROLLING ACCESS, BY AN AUTHENTICATION SERVER, TO PROTECTED

COMPUTER RESOURCES PROVIDED VIA AN INTERNET PROTOCOL NETWORK," issued on October 30, 2007 (Ex. 1, Filing No. 85),<sup>1</sup> from an application filed August 29, 2002, with the United States Patent and Trademark Office ("USPTO"). Prism contends that the '288 patent application<sup>2</sup> was a continuation-in-part of the application that matured into another Prism patent, U.S. Patent No. 6,516,416 ("'416 patent"), entitled "SUBSCRIPTION ACCESS SYSTEM FOR USE WITH AN UNTRUSTED NETWORK," which issued on February 4, 2003, from an application filed June 11, 1997 (Ex. 5, Filing No. 119).

The '345 patent, entitled "METHOD AND SYSTEM FOR MANAGING ACCESS TO PROTECTED COMPUTER RESOURCES PROVIDED VIA AN INTERNET PROTOCOL NETWORK" issued on February 28, 2012, from an application filed October 30, 2007, with the USPTO (Ex. 6, Filing No. 85). Prism contends that the '345 patent application was a continuation of the '288 patent application.

The '155 patent, entitled "SYSTEM FOR MANAGING ACCESS TO PROTECTED COMPUTER RESOURCES" issued on February 26, 2013, from an application filed November 11, 2010, with the USPTO (Ex. 7, Filing No. 85). Prism contends that the '155 patent application was a continuation of the '345 patent application.

---

<sup>1</sup> For ease of citation, the Court will cite to the filings in the AT&T Mobility LLC case (8:12CV122).

<sup>2</sup> The application for each issued patent will be referred to, for example, as "the '288 patent application," rather than by the patent application number.

The claims of the unasserted '416 patent include several of the same terms whose construction is now disputed in the presently asserted patents. In previous litigation initiated in 2005 by Prism against other defendants (the "Delaware Case"), the United States District Court for the District of Delaware (the "Delaware Court") construed the term "hardware key" and several other terms in the '416 patent that are also common to the asserted patents. (*Prism Tech. LLC v. Verisign, Inc.*, No. 1:05-214-JJF, Filing No. 449 (D. Del. Apr. 2, 2007) (Ex. 11, Filing No. 119, at 3 (the "Delaware Order")). See also *Prism Tech. LLC v. Verisign, Inc.*, 512 F. Supp. 2d 174 (D. Del. 2007), *aff'd*, 263 F. App'x 878 (Fed. Cir. 2008) (the "Delaware Memorandum"). Prism disclosed the Delaware Memorandum and the Delaware Order to the USPTO (see '288 patent, p. 15).

Prism appealed the Delaware Order, which the Federal Circuit affirmed without comment. Prism did not, however, appeal all of the claim constructions of the Delaware Order, and the constructions that it did appeal are not at issue in this case.

On December 29, 2008, Prism filed a complaint in this Court against defendants Research in Motion, Ltd. ("RIM") and Microsoft Corporation, alleging infringement of the '288 patent only (see Complaint, *Prism Tech. LLC v. Research in Motion et al.*, 8:08CV537 (the "RIM Case")). Although the case was settled before this Court held a *Markman* hearing or entered a claim

construction order, Prism and RIM did submit briefs in support of their proposed constructions.

On June 8, 2010, Prism filed a complaint in this Court against several software manufacturers, alleging infringement of the '288 patent only (see Complaint, *Prism Tech. LLC v. Adobe et al.*, 8:10CV220 (the "Adobe Case")). On April 11, 2011, the Court conducted an initial *Markman* hearing for the purpose of construing the term "hardware key / access key" and subsequently issued its claim construction order (Adobe Case, Filing No. 188 ("2011 Adobe Order")).

On January 12, 2012, the Court conducted a second *Markman* hearing in the Adobe Case for the purpose of construing additional disputed claim terms in the '288 patent. After the second *Markman* hearing, the parties in the Adobe Case submitted a joint stipulation on claim construction, including an agreement as to the significance of claim preambles and as to the definitions of five claim terms. The Court adopted the jointly stipulated agreement, and the Court construed the eight remaining disputed terms (Adobe Case, Filing No. 469 ("2012 Adobe Order")). Prism disclosed the 2011 and 2012 Adobe Orders to the USPTO (see '155 patent at pp. 17-18).

Prism claims that the asserted patents all descend from the invention of the '416 patent, as noted above. In the Adobe Case, Prism described the "Background of the Patented Technology" to this Court as follows:

In early 1996, the Internet was still in its infancy. Prism Resources, a predecessor to Prism Technologies, LLC, was busy addressing the problematic security issues associated with the open Internet. At that time, most Internet businesses provided access to computer resources openly over the Internet. When companies needed to control access, they were forced to use costly private networks. This was largely an artifact of the Internet being created without security in mind.

Prism Resources endeavored to solve these security problems so that companies could enjoy cost savings by employing the low-cost Internet to replace higher-cost private networks. Prism developed a revolutionary solution for controlling access to computer resources over an open network like the Internet. This novel system enabled access to resources using a hardware key from which digital credentials necessary for authentication could be generated, derived or read. This allowed companies to effectively turn the insecure public Internet connection between two parties into the equivalent of a secure, private network at low cost. Prism Resources proceeded to patent its ideas.

(Adobe Case, Filing No. 178, at 6-7) (internal citations omitted).

Prism similarly described its invention to the Federal Circuit in an appellate brief in the Delaware Case: "Prism set out to solve this very problem by developing a revolutionary solution for controlling access to computer resources over an

untrusted network like the Internet. Prism's novel system enables access to resources using a hardware key that contains digital credentials necessary for authentication." Brief of Plaintiff-Appellant Prism Technologies LLC, *Prism Tech. LLC v. Verisign, Inc.*, 263 F. App'x 878 (Fed. Cir. 2008) (No. 2007-1315), 2007 WL 2956764 ("Prism Brief - Delaware Case"). "The invention turned the insecure public Internet connection between two parties into the equivalent of a secure, low-cost private network." *Id.*

Prism filed its complaint in the present action on April 4, 2012 (Filing No. 1), which it amended on September 21, 2012 (Filing No. 40), and March 1, 2013 (Filing No. 85). On April 23, 2013, the parties filed a Joint Claim Construction Statement delineating their proposed claim constructions and stipulations (Filing No. 110).

## **II. Legal Standard.**

"It is a 'bedrock principle' of patent law that 'the claims of a patent define the invention to which the patentee is entitled the right to exclude.'" *Phillips v. AWH Corp.*, 415 F.3d 1303, 1312 (Fed. Cir. 2005) (en banc) (quoting *Innova/Pure Water, Inc. v. Safari Water Filtration Sys., Inc.*, 381 F.3d 1111, 1115 (Fed. Cir. 2004)). In construing a claim term, the Court must give each term its "ordinary and customary meaning, as [it] would be understood by one of ordinary skill in the art in question at the time of the invention." *Intervet Inc. v. Merial Ltd.*, 617

F.3d 1282, 1287 (Fed. Cir. 2010) (citing *Phillips*, 415 F.3d at 1312-13).

Because the meaning of a claim term as understood by persons of skill in the art is often not immediately apparent, and because patentees frequently use terms idiosyncratically, the court looks to "those sources available to the public that show what a person of skill in the art would have understood disputed claim language to mean."

*Phillips*, 415 F.3d at 1314 (quoting *Innova/Pure Water*, 381 F.3d at 1116). "Sources available to the public" include: (1) the patent claims themselves; (2) the remainder of the patent's specification; (3) the patent's prosecution history; and (4) extrinsic evidence pertaining to relevant scientific principles, such as a technical term's meaning and the state of the art.

*Phillips*, 415 F.3d at 1314.

"First, we look to the words of the claims themselves, both asserted and nonasserted, to define the scope of the patented invention." *Vitronics Corp. v. Conceptronic, Inc.*, 90 F.3d 1576, 1582 (Fed. Cir. 1996). "The written description part of the specification itself does not delimit the right to exclude. That is the function and purpose of claims." *Markman v. Westview Instruments, Inc.*, 52 F.3d 967, 980 (Fed. Cir. 1995), aff'd, 517 U.S. 370 (1996).

"Because claim terms are normally used consistently throughout the patent, the usage of a term in one claim can often

illuminate the meaning of the same term in other claims.” *Phillips*, 415 F.3d at 1314. “Where claims use different terms, those differences are presumed to reflect a difference in the scope of the claims.” *Forest Labs., Inc. v. Abbott Labs.*, 239 F.3d 1305, 1310 (Fed. Cir. 2001).

As to patent families, when “patents all derive from the same parent application and share many common terms, we must interpret the claims consistently across all asserted patents.” *NTP, Inc. v. Research in Motion, Ltd.*, 418 F.3d 1282, 1293 (Fed. Cir. 2005). “[W]e presume, unless otherwise compelled, that the same claim term in the same patent or related patents carries the same construed meaning.” *Omega Eng’g, Inc. v. Raytek Corp.*, 334 F.3d 1314, 1334 (Fed. Cir. 2003).

In addition to the language of the claims, the patent specification “is always highly relevant to the claim construction analysis. Usually, it is dispositive; it is the single best guide to the meaning of a disputed term.” *Phillips*, 415 F.3d at 1315 (quoting *Vitronics*, 90 F.3d at 1582). “Importantly, the person of ordinary skill in the art is deemed to read the claim term not only in the context of the particular claim in which the disputed term appears, but in the context of the entire patent, including the specification.” *Phillips*, 415 F.3d at 1313. After all, as required by statute,

The specification shall contain a written description of the invention, and of the manner and

process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same, and shall set forth the best mode contemplated by the inventor or joint inventor of carrying out the invention.

35 U.S.C. § 112(a).

"Statements that describe the invention as a whole, rather than statements that describe only preferred embodiments, are more likely to support a limiting definition of a claim term." *C.R. Bard, Inc. v. U.S. Surgical Corp.*, 388 F.3d 858, 864 (Fed. Cir. 2004). Because "the specification often describes very specific embodiments of the invention, we have repeatedly warned against confining the claims to those embodiments." *Phillips*, 415 F.3d at 1323. While

[t]he written description and other parts of the specification, for example, may shed contextual light on the plain and ordinary meaning[,] . . . they cannot be used to narrow a claim term to deviate from the plain and ordinary meaning unless the inventor acted as his own lexicographer or intentionally disclaimed or disavowed claim scope.

*Aventis Pharm. Inc. v. Amino Chem. Ltd.*, 715 F.3d 1363, 1373 (Fed. Cir. 2013). Thus "[t]he longstanding difficulty is the contrasting nature of the axioms that (a) a claim must be read in view of the specification and (b) a court may not read a

limitation into a claim from the specification." *Innova*, 381 F.3d at 1117.

After the claims themselves and the remainder of the specification, "[t]he court has broad power to look as a matter of law to the prosecution history of the patent in order to ascertain the true meaning of language used in the patent claims . . . ." *Markman*, 52 F.3d at 980. "This history contains the complete record of all the proceedings before the [USPTO], including any express representations made by the applicant regarding the scope of the claims. As such, the record before the [USPTO] is often of critical significance in determining the meaning of the claims." *Vitronics*, 90 F.3d at 1582. "[T]he prosecution history can often inform the meaning of the claim language by demonstrating how the inventor understood the invention and whether the inventor limited the invention in the course of prosecution, making the claim scope narrower than it would otherwise be." *Phillips*, 415 F.3d at 1317.

"The public notice function of a patent and its prosecution history requires that a patentee be held to what he declares during the prosecution of his patent." *Springs Window Fashions LP v. Novo Indus., L.P.*, 323 F.3d 989, 995 (Fed. Cir. 2003). "A patentee may not state during prosecution that the claims do not cover a particular device and then change position and later sue a party who makes that same device for infringement." *Id.* "'The purpose of consulting the prosecution

history in construing a claim is to exclude any interpretation that was disclaimed during prosecution.'" *Id.* (quoting *Chimie v. PPG Indus., Inc.*, 402 F.3d 1371, 1384 (Fed. Cir. 2005)).

### **III. Claim Construction.**

"When the parties present a fundamental dispute regarding the scope of a claim term, it is the court's duty to resolve it." *O2 Micro Int'l Ltd. v. Beyond Innovation Tech. Co., Ltd.*, 521 F.3d 1351, 1362 (Fed. Cir. 2008). Here, the Court finds that the parties have agreed that three terms, "internal," "client computer device" and "provided via . . .," should be "given their ordinary and customary meaning." *Phillips*, 415 F.3d at 1312. Since the parties do not "present a fundamental dispute," the terms do not require a construction from the Court.<sup>3</sup> The parties offer differing proposed constructions for the remaining terms on Schedule A, as follows.

- A. "Internet Protocol network"** terms ("an Internet Protocol network," "network utilizing at least one Internet Protocol," and "a network utilizing at least one Internet Protocol")

---

<sup>3</sup> See Schedule A, Filing No. 110 (For the three terms, plus the term "external," Prism states, "No construction is required -- plain and ordinary meaning"); Filing No. 114, at 19 n. 11 (Defendants state that the same terms "should be given their plain and ordinary meaning"). Nevertheless, the Court does choose to construe the term "external" (see "hardware key," below).

Prism's Proposed Construction:	Defendants' Proposed Construction:
"A network using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, and HTTP"	"An untrusted network using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, and HTTP/IP, where untrusted is defined as a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous"

Prism's proposed construction is the same as the construction to which the parties jointly stipulated for the '288 patent in the Adobe Case. Generally, claim terms from related patents (and certainly from the same patent) are interpreted consistently. *NTP*, 418 F.3d at 1293; *Omega Eng'g*, 334 F.3d at 1334. Defendants contend that because they were not a party to the stipulation adopted in the Adobe Case, and because they do not agree with the stipulation, the Court should place less significance on the previous construction.

Addressing a similar situation, the Federal Circuit wrote, "The infringement analysis in the initial determination was made pursuant to a stipulation with respect to the meaning of the claim terms by one of the respondents in that proceeding."

*Fuji Photo Film Co., Ltd. v. Int'l Trade Comm'n*, 386 F.3d 1095, 1101 (Fed. Cir. 2004). "Since the respondents who are affected by the claim construction in the present proceedings were not parties to that stipulation, they are not bound by it, nor does

the administrative law judge's acceptance of the stipulation constitute a formal claim construction." *Id.* Similarly, the Court will view the Adobe Case constructions based on stipulations as relevant (particularly because they appear in the prosecution history) but not binding to the present action.

The primary difference<sup>4</sup> between the parties' proposed constructions is defendants' insertion of the word "untrusted," defined in the '288 patent specification ('288 patent, 3:39-42).<sup>5</sup> Defendants contend that the "Internet Protocol network" terms as used in the asserted patents' claims should be restricted to untrusted networks; Prism claims that no such limitation exists. While Prism concedes that the '416 patent "generally claims systems for controlling the operation and access to protected resources where the access server and client computer communicate over an untrusted network," Prism contends that "claims in the '288 patent apply to both trusted and untrusted networks" (Filing No. 118, at 12).

---

<sup>4</sup> One other difference exists: Prism includes the term "HTTP," while defendants include the term "HTTP/IP." None of the parties has addressed this difference, and the Court has no way to determine the technical significance, if any, of the addition of "/IP." The Court will include both "HTTP" and "HTTP/IP" in its construction.

<sup>5</sup> The parties state that the specifications of the asserted patents are identical (see Filing No. 118, at 9 n.7; Filing No. 114, at 15). The Court will cite to the '288 patent specification only, but such citations apply similarly to the '345 patent and the '155 patent specifications.

**1. The Claim Language.** Prism states, “[B]y its plain language ‘an Internet Protocol network’ is a network that uses the Internet Protocol. As the claim language broadly recites ‘network’ without further limitation, as a matter of law, the claim captures any network, including both trusted and untrusted networks” (Filing No. 118, at 36).

Defendants read the claims differently; they propose that an “Internet Protocol network” is a subset of all untrusted networks (Defendant Slide 41). For example, claim 62 of the ‘288 patent begins as follows:

**62.** A method for protecting resources of a server computer, the server computer providing the protected resources to a client computer device via an untrusted network . . .

(‘288 patent, 39:48-50). Dependent claim 81 then reads,

**81.** The method of claim **62**, wherein the untrusted network uses an IP protocol.

(*Id.*, 41:39-40). Similarly, claim 87 begins,

**87.** A method for protecting resources of a server computer, the server computer providing the protected resources to a client computer device via an untrusted network . . .

(*Id.*, 41:61-63). Dependant claim 110 then reads,

**110.** The method of claim **87**, wherein the untrusted network uses an IP protocol.

(*Id.*, 43:63-64). Here, defendants persuasively argue that in the context of the '288 patent claims, networks that use an IP protocol are one species of untrusted network.

But Prism also contends that the doctrine of claim differentiation supports its argument. For example, Prism compares the preamble of claim 31, which contains the term "untrusted network," as cited above, with the preamble of claim 117, which contains the term "Internet Protocol network:"

**117.** A system for controlling access to protected computer resources provided via an Internet Protocol network . . .

(*Id.*, 45:1-2). Prism states, "The fact that the inventors of the Asserted Patents chose to use the term 'untrusted network' in some claims and 'Internet Protocol network' in others demonstrates that these terms must have different meanings based on the doctrine of claim differentiation" (Filing No. 118 at 37).

Defendants dispute the fact that the doctrine of claim differentiation applies in this case, because the two preambles have other differences unrelated to "untrusted network" and "Internet Protocol network" (Filing No. 126, at 15). Yet even if the doctrine of claim differentiation did apply, it does not address the disagreement between the parties, because the difference between the two terms is in dispute. Prism argues that the terms are different because an "Internet Protocol network" can be either trusted or untrusted; defendants argue that the terms are different because an "Internet Protocol

network" is a subset of the term "untrusted network." Thus the doctrine of claim differentiation does not aid the analysis.

## **2. Specification Disclosure.**

"Where the specification makes clear that the invention does not include a particular feature, that feature is deemed to be outside the reach of the claims of the patent, even though the language of the claims, read without reference to the specification, might be considered broad enough to encompass the feature in question."

*Thorner v. Sony Computer Entm't Am. LLC*, 669 F.3d 1362, 1366 (Fed. Cir. 2012) (quoting *SciMed Life Sys., Inc. v. Advanced Cardiovascular Sys., Inc.*, 242 F.3d 1337, 1341 (Fed. Cir. 2001)). "Generally, a claim is not limited to the embodiments described in the specification unless the patentee has demonstrated a clear intention to limit the claim's scope with words or expressions of manifest exclusion or restriction. . . . By the same token, not every benefit flowing from an invention is a claim limitation." *i4i Ltd. P'ship v. Microsoft Corp.*, 598 F.3d 831, 843 (Fed. Cir. 2010) (quotation and citation omitted), aff'd, 131 S. Ct. 2238 (2011).

Prism and defendants agree that the specification addresses both trusted and untrusted networks. Prism, however, contends that the network above the firewall in Figure 1 can be either trusted or untrusted, whereas defendants contend that the network above the firewall is untrusted only.

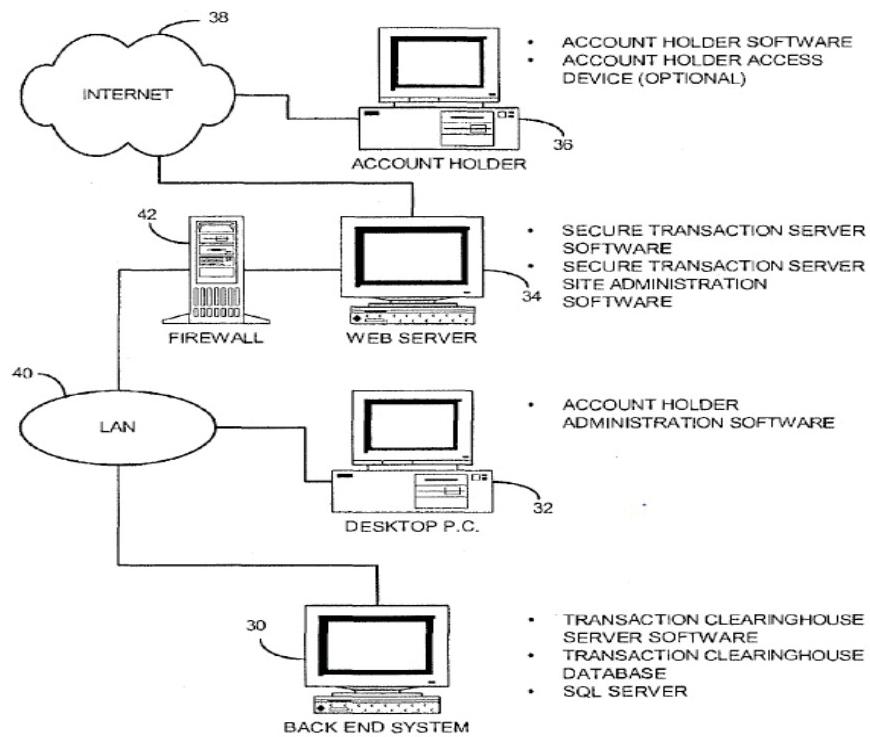


FIG. 1

(‘288 patent, Fig. 1).

At oral argument, defendants emphasized the fact that “[a]s the preamble to the asserted claims makes clear, the relevant ‘network’ is the network over which protected resources are ‘provided’ to a client computer device . . . .” (Defendants’ Slide 30, quoting ‘288 patent, claim 117). Defendants argue, “The preamble tells us that the network we’re looking at is the network that’s used to provide access to the protected computer resources by the client computer device. It’s the top half of Figure 1, not the bottom half” (*Markman Hearing Transcript, Filing No. 130, at 62:8-11*). Defendants argue that the “Internet

Protocol network" of claim 117 must correspond to INTERNET **38** of Figure 1, which connects ACCOUNT HOLDER **36** to WEB SERVER **34** (Defendants' Slide 30, quoting '288 patent, Fig. 1). Defendants also conclude that the term "Internet Protocol network" cannot be part of the trusted network indicated by solid lines in Figure 3, but that the term only refers to the part of the invention that is in the shape of the cloud and that connects the two sides of the drawing with dotted lines (Defendants' Slides 38-41).

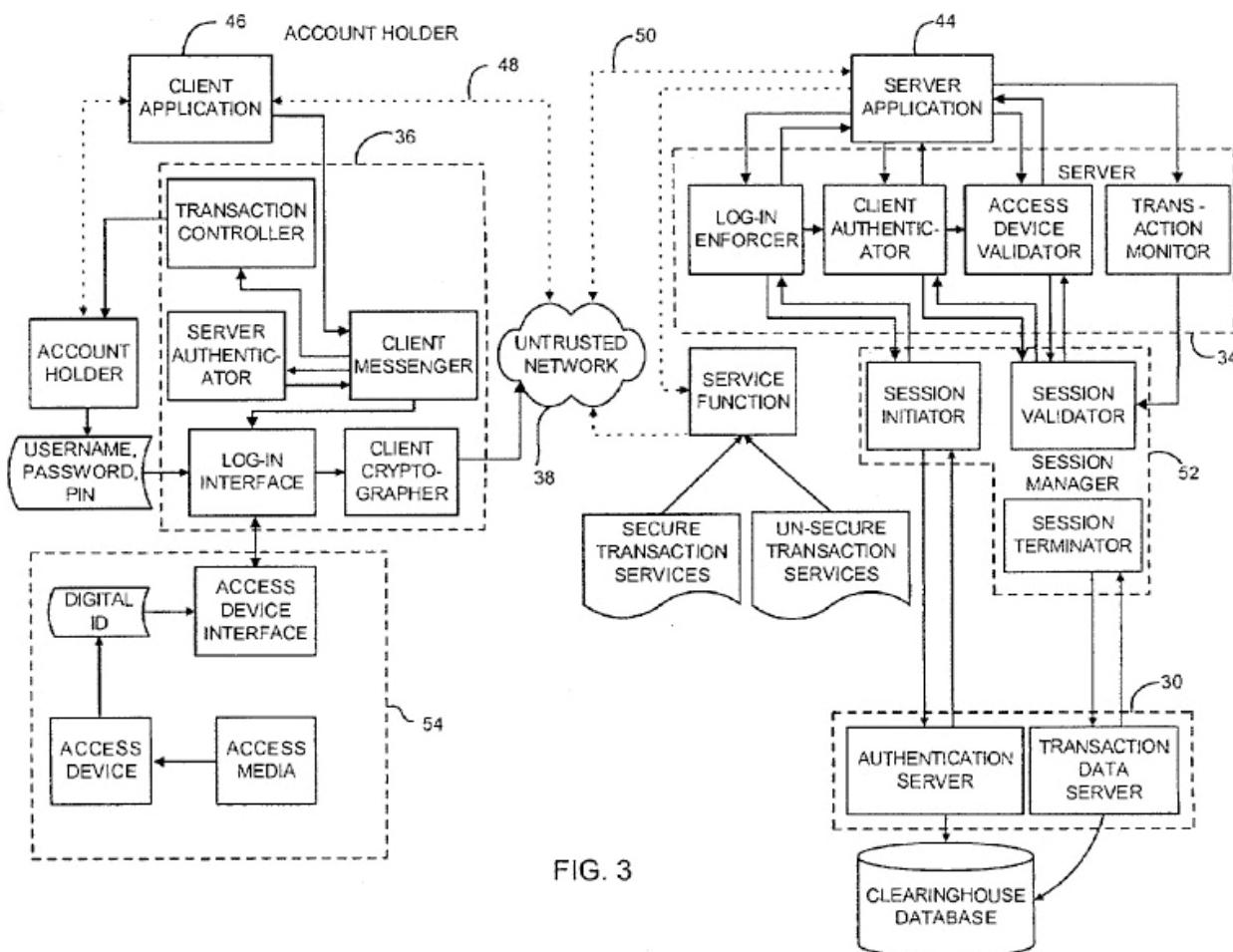


FIG. 3

('288 patent, Fig. 3).

Keeping in mind that some of the networks described in the specification are trusted and secure (illustrated by the solid lines in Figure 3), Prism's argument can be condensed as follows:

1. Some aspects of such a trusted and secure network, such as a LAN [local area network] use a TCP/IP protocol (Filing No. 124, at 13).
2. A network that uses a TCP/IP protocol is an "Internet Protocol network" (Plaintiff's Construction, Schedule A, Filing No. 110).
3. Therefore, the trusted and secure network that uses a TCP/IP protocol is an "Internet Protocol network," and an "Internet Protocol network" includes trusted networks.

(See Filing No. 118, at 36-37; Filing No. 124, at 12-14). This argument only succeeds if the second statement is true, that is, that a network that uses a TCP/IP protocol is an "Internet Protocol network." Yet this is the very position that Prism is setting out to prove; as such, it cannot be assumed. After all, defendants would rewrite the second statement as "An untrusted network that uses a TCP/IP protocol is an "Internet Protocol network," thereby not allowing for Prism's third, conclusory statement. Moreover, as defendants point out, "[t]he specification's disclosure of the LAN is irrelevant to the 'Internet Protocol network' terms because the LAN is not the network over which protected computer resources are provided from the access server to the client computer device as the preamble requires" (Filing No. 126, at 10-11).

Turning to the written language of the specifications, the first sentences of the '288 patent specification read as follows: "*The present invention generally relates to security systems for use with computer networks. More particularly, the present invention relates to a secure transaction system that is particularly adapted for use with untrusted networks, such as the Internet*" ('288 patent, 1:8-12) (emphasis added).

Describing the drawings, the specification reads, "FIG. 1 is a block diagram of the secure transaction system embodying *the present invention*, wherein a secure transaction server is part of a local area network, with the server being connected to the Internet and to the local area network via a firewall" (*Id.*, 2:17-21) (emphasis added). Also describing the drawings, "FIG. 3 is a more detailed block diagram of the schema of *the present invention*" (*Id.*, 2:26-27) (emphasis added).

The first sentences of the Detailed Description section of the '288 patent specification read as follows:

Broadly stated, *the present invention* is directed to a secure transaction system that is particularly adapted for use with an untrusted network, such as the Internet worldwide web. As used herein, an untrusted network is defined as a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous. A client-server application running over such a network has no control over the transmitted information during all

the phases of transmission. *The present invention provides a platform for securing transactions between consumers and suppliers on an untrusted network.*

(*Id.*, 3:36-46) (emphasis added). Finally,

While the steps that have been described with respect to FIG. 2 are a very broad overview of the preferred embodiment, the functional block diagram of FIG. 3 provides a more detailed general schema of *the present invention*. The system includes a server application 44, an account holder or client application 46, both of which are connected to an untrusted network via a traditional communication path indicated by the dotted lines 48 and 50.

(*Id.*, 6:24-31) (emphasis added).

The parties emphasize different aspects of the foregoing specification excerpts. Prism states, "The Specification uses the words 'present invention' in a permissive and general manner to describe the advantages of the claimed invention . . ." (Filing No. 124, at 14). Prism goes on to say, "The specification also provides examples of particular uses of the invention, such as '**particularly** adapted for use with untrusted networks, such as the Internet' and '**particularly adapted** for use with an untrusted network, such as the Internet worldwide web.' Such statements do not limit the scope of 'Internet Protocol networks'" (*Id.*, at 15).

Prism cites *i4i* to support its contention that a description of a "particular advantage" of an invention does not limit the invention (*Id.*). Prism claims, "[T]he permissive language used in the Specification (e.g., 'generally,' 'particularly adapted,' 'broadly stated,' 'provides a platform,' 'general schema') is not limiting" (*Id.*, at 16). Prism likens these terms to terms in the *i4i* patent specification that the Federal Circuit did find to be permissive: "The specification's permissive language, 'could be edited,' 'can be created,' and 'ability to work,' does not clearly disclaim systems lacking these benefits." *i4i*, 598 F.3d at 844.

The Court does not find Prism's language to be permissive in the same sense as "can be" and "could be," which create a possibility but not a requirement. The specification itself distinguishes between Figure 2, showing "a very broad overview of the preferred embodiment," and Figure 3, showing "a more detailed general schema of the present invention." The Court finds that the plain language of these statements indicates that Figure 3 is not, in fact, a particular advantage or a preferred embodiment like Figure 2, but rather is just as Prism describes it -- a "general schema of the present invention," with no permissive language present at all.

Defendants emphasize Prism's use of the term "the present invention," citing *Honeywell*, where the Federal Circuit found that "the claim term 'fuel injection system component' is

limited to a fuel filter." *Honeywell Int'l, Inc. v. ITT Indus., Inc.*, 452 F.3d 1312, 1318 (Fed. Cir. 2006). In arriving at this limitation, the Federal Circuit cited four instances in the patent's specification where "the written description refers to the fuel filter as 'this invention' or 'the present invention . . . .'" *Id.* The Federal Circuit concluded that under such circumstances, "[t]he public is entitled to take the patentee at his word and the word was that the invention is a fuel filter." *Id.*

Prism cites *Martek Biosciences Corp. v. Nutrinova, Inc.*, 579 F.3d 1363 (Fed. Cir. 2009) as an example of the rejection of a claim limitation based on a description of "the present invention." But in *Martek*, the patentee had acted as its own lexicographer with regard to the claim term in question, which is not the case here. ("When a patentee explicitly defines a claim term in the patent specification, the patentee's definition controls." *Id.* at 1380.)

In consideration of the foregoing, the Court finds that defendants have persuasively argued that the specification is dispositive on the issue and that, as in *Honeywell*, the specification speaks for itself as to the untrusted nature of the network connection between the client computer device and the server that allows for access to protected computer resources.

**3. Prosecution History Disclaimer.** "We indulge a heavy presumption that claim terms carry their full ordinary and

customary meaning unless the patentee unequivocally imparted a novel meaning to those terms or expressly relinquished claim scope during prosecution." *Omega Eng'g*, 334 F.3d at 1323 (Fed. Cir. 2003) (quotation and citations omitted). "[F]or prosecution disclaimer to attach, our precedent requires that the alleged disavowing actions or statements made during prosecution be both clear and unmistakable." *Id.* at 1325-26 (footnote omitted). "[A]n applicant can make a binding disavowal of claim scope in the course of prosecuting the patent, through arguments made to distinguish prior art references." *Cordis Corp. v. Medtronic Ave, Inc.*, 511 F.3d 1157, 1177 (Fed. Cir. 2008). "In order to constitute binding surrenders of claim scope, the statements in question must be such that 'a competitor would reasonably believe that the applicant had surrendered the relevant subject matter.'" *Id.* (quoting *Cybor Corp. v. FAS Tech., Inc.*, 138 F.3d 1448, 1457 (Fed. Cir. 1998) (en banc)).

Defendants contend that "Prism disclaimed a system that operates over a private, trusted network -- the same type of network that it now seeks to reclaim through its proposed construction of the terms 'Internet Protocol network' and 'network utilizing at least one Internet Protocol'" (Filing No. 114, at 20). "Because of this [prosecution] disclaimer, 'Internet Protocol network' and 'network utilizing at least one Internet Protocol' should be limited to an *untrusted network*" (*Id.*).

Defendants cite a document filed by Prism with the USPTO on January 19, 2000, during prosecution of the '416 patent, distinguishing prior art ("Dolphin") by stating, "With respect to the rejection of claims 1 and 28 as being anticipated by Dolphin reference, it is submitted that claims 1 and 28 are not anticipated . . ." (Ex. 4, Filing No. 118, at 8). "The Dolphin reference uses a private network for communications between the subscriber and the billing/access center designed to allow only subscribers to obtain the unique key material identifier (KMID) needed to decrypt the computer resources" (*Id.*). "Thus, it does not teach or suggest a system that includes, among other things, a clearinghouse means, server software means and client software means as claimed by *the present invention*" (*Id.*) (emphasis added).

Prism responds, "Rather than constitute a disclaimer, the [first sentence of the January 19, 2000, statement] is simply a statement of what the Dolphin reference teaches -- i.e., a private network for communications -- while the [second sentence], where Prism distinguishes Dolphin, does not mention that Dolphin is a private network" (Filing No. 124, at 11). "Indeed, Prism's Response relied entirely on other claimed limitations, such as the clearinghouse, server software means, and client software means to distinguish Dolphin . . ." (*Id.*).

But Prism clarified its statement to the USPTO when it stated to the Federal Circuit with regard to the Dolphin prior

art, "In response to this rejection, the applicants noted, inter alia, that Dolphin used a private, not a public (untrusted) network for communications between the subscriber and a billing access center that allows authenticated subscribers to obtain a key needed to decrypt the desired computer resources" (Prism Brief -- Delaware Case). "Thus, Dolphin taught neither server software means nor client software means functioning as described in Prism's application" (*Id.*). Prism's notable distinction between "a private [network]" and a "public (untrusted) network" suggests to the Court that Prism's statement to the Federal Circuit was not "simply a statement of what the Dolphin reference teaches," but rather a clear and unmistakable distinction between Dolphin's "private" network and Prism's "public (untrusted)" network. Prism's statement to the Federal Circuit lends credence to defendants' contention that such a distinction was also made to the USPTO.

The USPTO seemed to reach this conclusion as well. At oral argument, defendants noted that subsequent to Prism's January 19, 2000, statement, on September 21, 2000, the USPTO issued an Office Action stating, "Claims 1, 2, 4, 6-11, 15-17, 20, 22-24, 28 and 30-36 are allowed. The following is art examiner's statement of reasons for allowance: The present invention comprises a system for accessing subscription materials

over an unsecure network. . . ." (8:12CV123, Ex. 2, Filing No. 130, at 39; this document was not filed in 8:12CV122).<sup>6</sup>

Prism argues that even if prosecution history disavowal were to be found, any disclaimer would not apply to the downstream, asserted patents. Prism states, "Unlike the '416 patent [claims], the asserted claims here do not include the 'untrusted network' limitation and therefore any purported disclaimer from the prosecution of the '416 patent would not apply to claims in the later issued Asserted Patents" (Filing No. 124, at 12).

Yet the Federal Circuit advises that an important exception exists to the general rule: "We have explained that '[w]hen the purported disclaimers [made during prosecution] are directed to specific claim terms that have been omitted or materially altered in subsequent applications (rather than to the invention itself), those disclaimers do not apply.'" *Regents of Univ. of Minnesota v. AGA Med. Corp.*, 717 F.3d 929, 943 (Fed. Cir. 2013) (quoting *Saunders Grp., Inc. v. Comfortrac, Inc.*, 492 F.3d 1326, 1333 (Fed. Cir. 2007)). "In general, a prosecution disclaimer will only apply to a subsequent patent if that patent contains the same claim limitation as its predecessor." *Regents*, 717 F.3d at 943. "The sole exception is when the disclaimer is

---

<sup>6</sup> This document was first cited to the Court at oral argument; defendants did not cite to it in their briefs. Prism had been alerted to the possibility of such a citation but did not object at the hearing (See *Markman Hearing Transcript*, at 7:18-8:23; 65:12-66:10).

directed to the scope of the invention as a whole, not a particular claim. See, e.g., *Ormco Corp. v. Align Tech., Inc.*, 498 F.3d 1307, 1314-15 (Fed. Cir. 2007) (the patentee's statements 'w[ere] not associated with particular language from [the] claims' but were instead directed to the 'present invention' and the 'overall method' claimed)." *Regents*, 717 F.3d at 943, n.8. As in *Ormco*, here, where Prism's statement to the USPTO was directed to "the present invention," the exception applies as well -- that is, the disclaimer made during the '416 patent prosecution would apply to the downstream, asserted patents.

In consideration of the claim language, the specification, and the prosecution history,<sup>7</sup> considered in descending order of emphasis, the Court must reject Prism's contention that the term "Internet Protocol network" in the context of the asserted patents can apply more broadly, not only to public, untrusted networks, but also to private, trusted networks. While the network behind the firewall can certainly include a private, trusted, network, the Court must conclude that the "Internet Protocol network" by which the invention controls access to protected computer resources is untrusted.

---

<sup>7</sup> Because the Court finds the intrinsic evidence to be dispositive of the construction, the Court does not consider Prism's discussion of a patent not at issue here (Filing No. 124, at 21-23).

Accordingly, the Court is persuaded to amend its previously stipulated construction. The Court construes each of the “**Internet Protocol network**” terms (“**an Internet Protocol network**,” “**network utilizing at least one Internet Protocol**,” and “**a network utilizing at least one Internet Protocol**”) to mean “**an untrusted network using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, HTTP, and HTTP/IP, where untrusted is defined as a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous.**”

B. “**forward/receive**” terms (“forward,” “forwards,” and “forwarded”; “receive” and “receiving”)

Prism’s Proposed Constructions	Defendants’ Proposed Constructions
<p><b>“forward”:</b> Prism argues that no construction is required, and that the term should be given its plain and ordinary meaning.</p> <p><b>“receive”:</b> Prism argues that no construction is required, and that the term should be given its plain and ordinary meaning.</p>	<p><b>“forward”:</b> “transmit non-wirelessly”</p> <p><b>“receive”:</b> “receive non-wirelessly”</p>

While the terms “forward” and “receive” were not separately construed in the Delaware Case and the Adobe Case, both courts construed terms containing the term “forward.” In the Delaware Case, such terms were stipulated to by the parties

(Delaware Order, at 6, 7). More significantly, in the Adobe Case, after hearing argument by the parties, this Court construed "selectively requiring . . . [said/the] client computer device to forward" to mean "choosing to require that the client computer device transmit certain information," and the Court construed "adapted to forward" to mean "configured to transmit" (2012 Adobe Order, at 31-32). Thereby, the word "forward" was effectively construed as "transmit." Similarly, in this case, the parties have stipulated that the term "selectively requiring . . . [said/the] client computer device to forward" is construed as "choosing to require that the client computer device transmit certain information" (Filing No. 110, Schedule B). There too, the term "forward" is effectively construed as "transmit."

The debate here centers around defendants' proposed requirement of "non-wireless" transmission and reception, which Prism opposes. Prism notes that in the context of construing the term "hardware key" in the Delaware Case, the Delaware Court had occasion to state with regard to the term "connected,"

[E]ven though the inventors did not describe any embodiment of a hardware key that connects wirelessly to the computer, patent claims are not limited to only those features described in the specification, and later-developed technology is commonly allowed to be covered by broad claim terms.

*Varco, L.P. v. Pason Sys. USA Corp.*, 436 F.3d 1368, 1375-76 (Fed. Cir. 2006) (citing *SRI Int'l v. Matsushita Elec. Corp. Of Am.*, 775 F.2d 1107, 1121 (Fed. Cir. 1985)

(‘The law does not require [that] an applicant describe in his specification every conceivable and possible future embodiment of his invention.’) (*en banc*)). Thus, wireless devices are anticipated by the broad language in the claims and specification.

*Prism*, 512 F. Supp. 2d at 189. The “wireless device” cited by the Delaware Court was the hardware key only (see discussion of “hardware key” below). The Delaware Court did not address wireless communication between any of the invention’s other computers or servers.

**1. The Claim Language.** Looking first to the language of the claims themselves, defendants’ proposed construction would seem to be impossible. For example, dependent claim 136 of the ‘288 patent reads,

**136.** The system of claim 117, wherein said at least one client computer device wirelessly forwards said digital identification to said at least one access server.

(‘288 patent, 46:43-45). Likewise, dependent claim 170 reads,

**170.** The method of claim 150, wherein receiving, at the at least one access server, the digital identification from the at least one client computer device includes wirelessly receiving the digital identification.

(*Id.*, 49:1-4). As Prism points out, defendants’ construction, as applied to claim 136, would mean that the “client computer device wirelessly transmits non-wirelessly said digital identification,”

which would be nonsensical. Moreover, Prism argues that the doctrine of claim differentiation supports its argument in favor of both wireless and non-wireless transmission, in that the independent claims 117 and 150, which do not mention wireless transmission, are limited by dependent claims 136 and 170, which do, thereby meaning that the terms "forward" and "receive" can support both wireless and non-wireless transmission.

**2. Specification Disclosure.** As noted by the parties, the specification is largely silent on the issue of wireless vs. non-wireless transmission. Nonetheless, Prism does argue that the specification nowhere limits the terms "forward" and "receive" to non-wireless transmission. For example, with regard to Figure 3 above, the specification states that "the dotted lines are conventional communication paths," which Prism espouses could be wireless or non-wireless paths, which would have been known to a person of ordinary skill in the art at the time of the '416 prosecution in 1997 (Filing No. 118, at 28; see also '288 patent, 6:24-38).

In support of this contention, Prism introduces extrinsic evidence in the form of an article written in 1994 announcing, "AT&T will next month add roaming capabilities to its wireless WaveLAN network" (Ex. 15, Filing No. 119, at 2). Defendants, on the other hand, state that the same article supports their argument that "conventional communication paths" at the time would have been non-wireless: "The WavePoint

[wireless] bridge links WaveLAN to conventional wired networks" (*Id.*). Defendants also cite a patent claimed as prior art by Prism (which is, therefore, intrinsic evidence; see *Phillips*, 415 F.3d at 1317) in support of their position (Filing No. 126, at 24). On such scant evidence, the Court will not render a decision as to what constituted a conventional communication path in 1997.

**3. Prosecution History Disclaimer.** Defendants claim, "Because Prism disclaimed wirelessly transmitting and receiving during prosecution of the '155 Patent, these terms should be construed to mean transmitting and receiving non-wirelessly" (Filing No. 114, at 27). The purported disclaimer was made in response to a USPTO office action dated October 6, 2011, where USPTO Examiner Aubrey Wyszynski rejected submitted claims 1-20 in the '155 patent application (Ex. 7, Filing No. 117). Among the twenty rejected claims, two are relevant here:

3. The system of claim 1, wherein said at least one server is adapted to receive said identity data wirelessly.
14. The method of claim 12, wherein receiving, by the at least one server, the identity data from the at least one client computer device includes wirelessly receiving the identity data.

(Ex. 3, Filing No. 117, at ¶¶ 3, 14).

Examiner Wyszynski rejected all twenty claims for several reasons, including nonstatutory obviousness-type double patenting over claims 1-187 of the '288 patent and statutory obviousness rejections over prior art pursuant to 35 U.S.C. § 103(a) (Ex. 7, Filing No. 117, at 7, 10). Examiner Wyszynski also specifically rejected Claims 3 and 14, stating,

Claims 3 and 14 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the written description requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to reasonably convey to one skilled in the relevant art that the inventor(s), at the time the application was filed, had possession of the claimed invention. The examiner cannot find support in the specification for 'wireless' communication.

(Ex. 7, Filing No. 117, at 10).

On April 5, 2012, Prism responded to Examiner Wyszynski's rejections of the twenty claims by amending the '155 patent application to cancel claims 1-20, add new claims 21-117, and amend the title and abstract (Ex. 8, Filing No. 117). Prism specifically stated that it "cancelled claims 1-20 without prejudice or disclaimer of their subject matter" (*Id.* at 19). Prism stated that its cancellation of the claims rendered the examiner's rejections "on the ground of nonstatutory obviousness-type double patenting," "under 35 U.S.C. § 112, first paragraph," and "under 35 U.S.C. § 103(a)" "moot" (*Id.*). Defendants now

argue that Prism's cancellation of claims 3 and 14, particularly, amount to prosecution history disclaimer as to wireless communications, since one of the grounds on which Examiner Wyszynski cancelled the claims was lack of specification support for wireless communications.

"The doctrine of prosecution disclaimer is well established in Supreme Court precedent, precluding patentees from recapturing through claim interpretation specific meanings disclaimed during prosecution." *Omega Eng'g*, 334 F.3d at 1323. "'It is a rule of patent construction consistently observed that a claim in a patent as allowed must be read and interpreted with reference to claims that have been cancelled or rejected, and the claims allowed cannot by construction be read to cover what was thus eliminated from the patent.'" *Id.* (quoting *Schriber-Schroth Co. v. Cleveland Trust Co.*, 311 U.S. 211, 220-21 (1940)). "The injurious consequences to the public and to inventors and patent applicants if patentees were thus permitted to revive cancelled or rejected claims and restore them to their patents are manifest." *Schriber-Schroth*, 311 U.S. at 221.

"As a basic principle of claim interpretation, prosecution disclaimer promotes the public notice function of the intrinsic evidence and protects the public's reliance on definitive statements made during prosecution. We have, however, declined to apply the doctrine of prosecution disclaimer where the alleged disavowal of claim scope is ambiguous." *Omega Eng'g*,

334 F.3d at 1324 (internal citation omitted). "But where the patentee has unequivocally disavowed a certain meaning to obtain his patent, the doctrine of prosecution disclaimer attaches and narrows the ordinary meaning of the claim congruent with the scope of the surrender." *Omega Eng'g*, 334 F.3d at 1324.

For example, in *Rheox, Inc. v. Entact, Inc.*, 276 F.3d 1319, 1325, 61 USPQ2d 1368, 1373 (Fed. Cir. 2002), we ruled that the scope of the patent in suit did not cover 'triple superphosphate' - an embodiment expressly disclosed in the written description - because the patentee cancelled a claim covering 'triple superphosphate' and expressly disclaimed that compound in his arguments to the examiner to gain patent allowance.

*Id.* at 1324-25 (emphasis added).

The Federal Circuit describes another example of claim disavowal as follows: "The applicants disavowed claim coverage of sustained release tablets by cancelling original claims 1-11 and remarking to the examiner that '[o]riginal claims 1-11 were directed to a sustained release formulation. . . . [T]he sustained release claims have been cancelled to facilitate prosecution.'" *Reckitt Benckiser Inc. v. Watson Laboratories, Inc.*, 430 F. App'x 871, 876 (Fed. Cir. 2011) (internal citation omitted). "The unmistakable effect of that disavowal, evident from the applicants' remarks distinguishing the prior art, was to limit the remaining claims to two-portion guaifenesin products."

*Id.* In contrast, "There is no 'clear and unmistakable'

disclaimer if a prosecution argument is subject to more than one reasonable interpretation, one of which is consistent with a proffered meaning of the disputed term." *SanDisk Corp. v. Memorex Products, Inc.*, 415 F.3d 1278, 1287 (Fed. Cir. 2005).

The parties have not uncovered a case where a prosecution history disclaimer was alleged after the rejection of a claim on more than one ground, as here. In addition, as Prism points out, "All of Defendants' cases involved disclaimers where the patentee did not already have issued claims expressly directed toward the claim scope that was later argued to be disavowed" (Filing No. 124, at 25). "Here, by contrast, Prism already had issued claims expressly directed towards wireless communications -- the claim scope that Defendants argue Prism disavowed" (*Id.*).

Defendants suggest that nothing in the file wrapper indicates that the examiner looked at the issue carefully ("'[W]ireless' only came in at the very tail end [of the '288 patent prosecution] after . . . the bulk of the issues were resolved, as two dependent claims, as part of 75 new claims that were then summarily allowed two months later") (*Markman Hearing Transcript*, at 81:7-11). Defendants argue, "Prism could have opposed [Examiner Wyszynski's] rejection by making the same argument it raises here -- that two 'wireless' dependent claims were approved by a prior examiner of the '288 Patent" (Filing No. 126, at 22). "Instead, Prism failed to challenge the Examiner's

clear statement about the scope of the patents, and canceled its pending wireless claims. That is the essence of disclaimer" (*Id.* (internal citation omitted)). The Court disagrees.

The Court finds that Prism's strong arguments in favor of its construction, made largely by examination of the claims themselves, are not overcome by defendants' argument in favor of prosecution history disavowal. Prism did not clearly and unmistakably disavow wireless transmission when it cancelled original claims 3 and 14 of the '155 patent application. Prism's cancellation is subject to more than one reasonable interpretation, since claims 3 and 14 were also rejected by the examiner on grounds unrelated to wireless transmission. Similarly, Prism did not "expressly disclaim[] [wireless transmission] in [its] arguments to the examiner to gain patent allowance." *Omega Eng'g*, 334 F.3d at 1324-25. The Court will not impose a "non-wireless" limitation on the terms "forward" and "receive."

In keeping with the Court's previous constructions of phrases including the term "forward" in the Adobe Case, and in consideration of the parties' stipulation in this case, the Court construes "**forward**" to mean "**transmit**." The Court will not construe the word "**receive**" but will give it its plain and ordinary meaning.

C.     **"Protected Computer Resources"** terms ("protected computer resources," "protected resources," and "protected resources of at least one server computer")

Prism's Proposed Construction:	Defendants' Proposed Construction:
"Computer services, applications, or content that can be accessed (either directly or indirectly)"	"Computer services, applications, or content that is stored within the secure transaction system that can only be accessed by a server within the secure transaction system"

Like the Internet Protocol network terms, Prism's proposed construction for the protected computer resources terms is the same as the construction to which the parties jointly stipulated for the '288 patent in the Adobe Case. As with the Internet Protocol network terms, the Court will view the Adobe Case construction as relevant but not binding to the present actions.

Prism also emphasizes the fact that the Delaware Court construed the term "selected computer resources of at least a [or said] first server computer" from the '416 patent to mean "computer services, applications, or content that can be accessed by (either directly or indirectly) said first server computer" (Delaware Order, at 2), supporting Prism's construction here. Defendants recall the doctrine of claim differentiation, arguing that "'protected' is presumed to have a different meaning from 'selected,' and the proper construction of 'protected resources'

turns on that difference" (Filing No. 126, at 20). The Court agrees that the words "selected" and "protected" have different meanings, and the Court assumes that the inventors used different terms to convey different meanings.

**1. The Claim Language.** Unlike Prism's construction, defendants' construction has two additional requirements: first, that the protected resources be "stored within the secure transaction system," and second, that the protected resources "can only be accessed by a server within the secure transaction system." Defendants state, "Prism's proposed construction would render the word 'protected' superfluous. Indeed, under Prism's construction, 'protected resources' can be *any* computer resource accessible by *any* means" (Filing No. 114, at 30). Defendants continue, "[U]nder Prism's construction, a popular website outside of Defendants' control and publicly available to anyone with an internet connection, such as www.google.com, would be considered a 'protected computer resource'" (*Id.*, at 30 n.16).

On the other hand, Prism states that "there is nothing in the asserted patent claims, Specification, or prosecution history that requires the 'protected resources' or 'protected computer resources' to be stored in any particular location or only be accessible by a server within the secure transaction system" (Filing No. 118, at 34). In addition,

When Prism's construction is read in the context of the claims, protected resources refers only to

resources made available to a client computer device after the client computer device is authenticated and authorized to access the protected resources — that is, the required authentication and authorization pathway is what makes the resources protected.

(Filing No. 124, at 29). In fact, "Internet access itself could be the protected resource" (*Markman Hearing Transcript*, at 103:14).

**2. Specification Disclosure.** In the RIM Case, Prism assisted the Court in its understanding of the '288 patent specification by providing an annotated Figure 3:

In its most basic form, the security system comprises four elements, those being: (1) an access server (34 purple), (2) a client computer device (54 pink), (3) a hardware key associated with the client computer device (36 orange), and (4) an authentication server (30 green). These elements (or steps in the method claims) are adapted to permit access to the protect computer resources (yellow) upon successful authentication and authorization. Figure 3 of the patent sets forth a very basic overview of the invention:

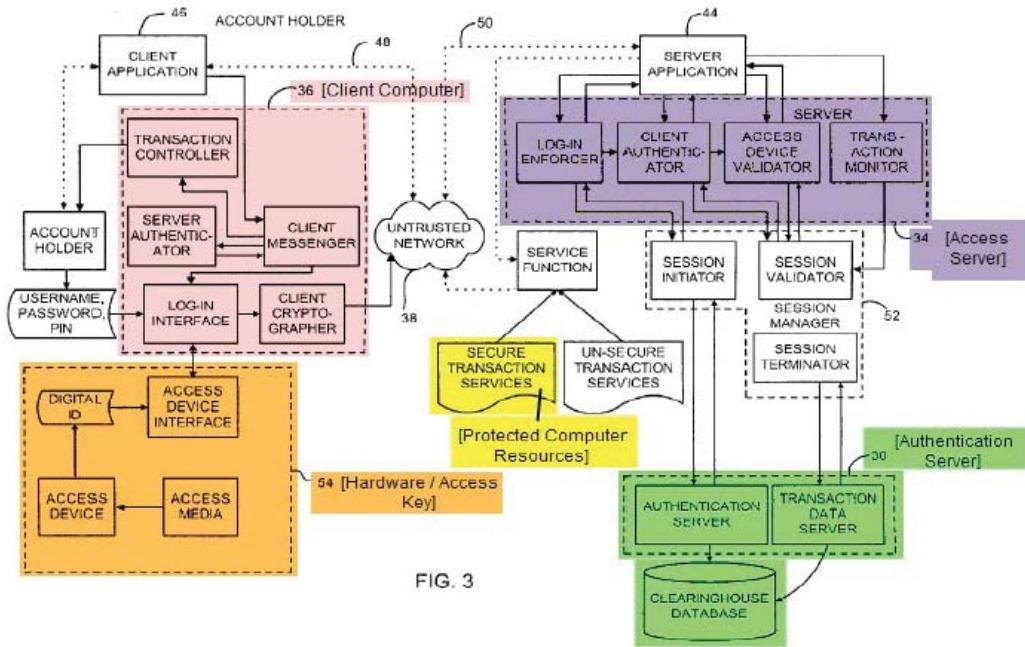


FIG. 3

(RIM Case, Filing No. 76, at 6-7) (internal citations omitted).

Thus Prism indicated to this Court that the protected computer resources were located at the "secure transaction services."

Prism specifically did not indicate that the protected computer resources were located at the "un-secure transaction services," immediately to the right of the secure transaction services.

From this, defendants argue that "Prism's construction in this case allows the claimed 'protected computer resources' to be any service, application, or content accessed in any way, including the 'un-secure transaction services' that Prism excluded previously" (Filing No. 114, at 34).

Further, Prism told this Court,

The purpose of the invention is to secure access to the "protected

computer resources.” Protected computer resources include computer services, applications, content, files, data or other information. The invention controls access to the protected content through an authentication and authorization process utilizing an access server [item 34] and authentication server [item 30]. Importantly, the protected resources may be located at the access server itself, or remotely at other servers or databases which are directly or indirectly accessible to the access server.

(RIM Case, Filing No. 76, at 7). Prism did not suggest to the Court that the “other servers or databases” wherein the “protected resources may be located” are *someone else’s* servers or databases, nor did it suggest that the “other servers or databases” are outside of the invention entirely. The specification states, “The account holder software **36** is installed on the account holder’s personal computer. This software enables a web browser **77** to access the transaction services **78** provided by the secure transaction server” (‘288 patent, 8:56-59). Hence the secure transaction services **78**, where the protected resources are located, are “provided by the secure transaction server,” not some outside server.

Defendants emphasize this point by stating, “The specification only describes a system that provides computer resources (*i.e.*, ‘transaction services’) that are stored within the servers and computer systems of the company that hosts the

secure transaction system . . ." (Filing No. 114, at 31).

Defendants point out that the specification teaches,

A web master or a system administrator needs to determine which transactions are to be protected and make sure that all these transactions are organized in separate directories from unprotected transaction services. In this way, the web server configuration can be changed to protect these particular directories using the secure transaction system.

('288 patent, 11:20-26). The specification also states, "The administration software **64** allows an administrator to define the particular transaction services that can be accessed by an account holder" (*Id.*, 10:40-42). This would not seem to be possible if the protected computer resources ("particular transaction services") are located outside of the invention.

Prism emphasizes the importance of the Delaware Court's construction of the term including "selected computer resources," on which Prism's proposed construction is based (Filing No. 118, at 34). Prism claims that the Delaware Court "specifically rejected construing a related term ('selected computer resources') in the '416 patent to include the limitation that the protected resources need be stored in a particular location as Defendants argue here" (*Id.*). On this point, the Delaware Court stated,

The specification discusses a system whereby various web sites are hosted through web servers operating in conjunction with first server computers<sup>8</sup> that protect the contents of the sites. Figure 3 shows the protected contents *residing outside of the first server computer*, with the path over which protected contents can be sent crossing through the 'Service Function' block rather than the server. Likewise, in Figure 4, the protected content resides *outside the first server*, and is accessed by the server through the 'Service Function,' which also resides *outside the first server computer*. Thus, the Court concludes that the system disclosed in the specification and corresponding figures does not require the first server computer to store the resources it communicates to subscribers. Rather, it allows the server to act as a gatekeeper, accessing *selected computer resources protected by the invention* either itself or through a 'Service Function' block, and communicating those resources to subscribers.

*Prism*, 512 F. Supp. 2d at 186 (emphasis added) (internal citations omitted).

---

<sup>8</sup> Prism states that the asserted patent claims use the terms "server computer" and "access server" rather than the "first server computer" of the '416 patent. See Filing No. 118, at 34.

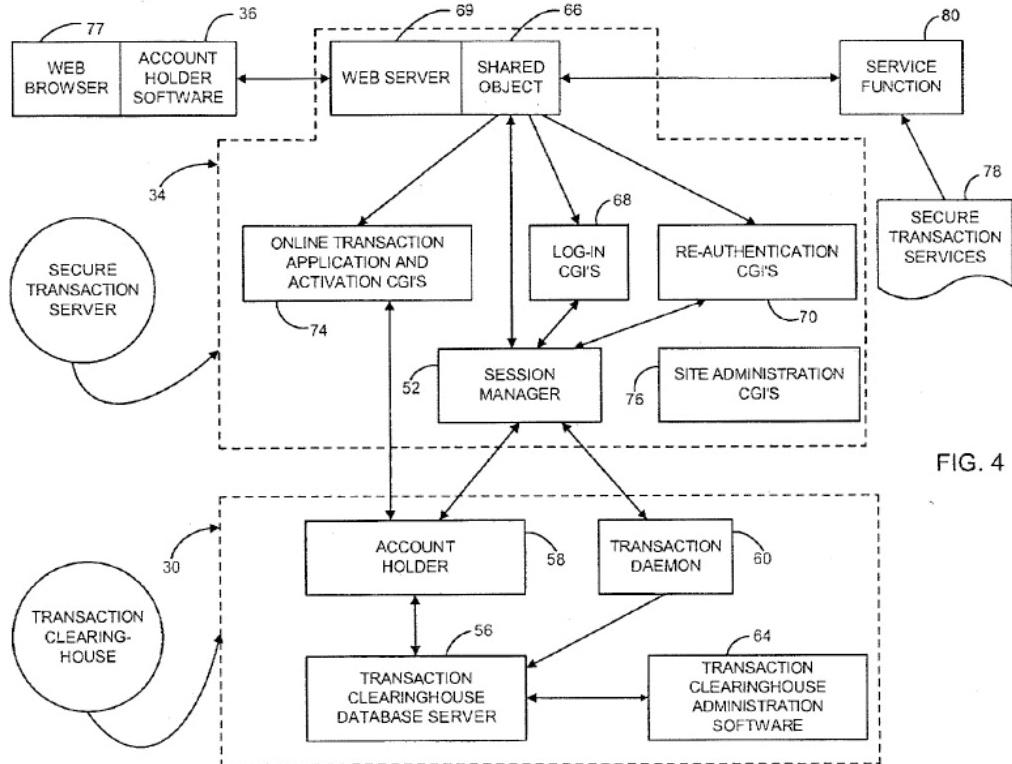


FIG. 4

('288 patent, Fig. 4).

The Court first notes that the Delaware Court was indeed construing a different term, "selected computer resources" rather than "protected computer resources." The dispute in the Delaware Case was as to whether the selected computer resources had to be located at the first server computer or whether they could be located on a server outside of the first server computer. *Prism*, 512 F. Supp. 2d at 185-86. Unlike defendants' construction in the Delaware Case, defendants' construction here does not specifically require a particular server to hold the protected computer resources; it only states that such a server is "within the secure transaction system."

While the Delaware Court did state that Figures 3 and 4 did not require the selected computer resources to be located on the first server computer, the Delaware Court did not go so far as to say that the selected computer resources or the web servers could be located outside of the secure transaction system. The Court takes Prism at its word when it located the protected computer resources at the secure transaction services, that is, at a location within the invention and provided by the secure transaction server.

In consideration of the claim language and the specification of the asserted patents, the Court is persuaded to amend its previously stipulated construction. The Court construes each of the "**protected computer resources**" terms ("**protected computer resources**," "**protected resources**," and "**protected resources of at least one server computer**") to mean "**Computer services, applications, or content that is stored within the secure transaction system that can only be accessed by a server within the secure transaction system.**"

**D. "digital identification"**

Prism's Proposed Construction:  "digital data whose value is known in advance or calculated [at] the moment"	Defendants' Proposed Construction:  "digital data stored on a hardware key / access key whose value is known in advance or calculated at the moment"
--	--

Here, Prism's construction of "digital identification" is identical to the Delaware Court's construction of the same term in the '416 patent and to this Court's construction of the same term in the '288 patent in the Adobe Case. Defendants' proposed construction differs in that it requires that the digital identification be "stored on a hardware key/access key."

As construed by the Court, a hardware key / access key is "an external hardware device or external object from which the predetermined digital identification can be read" (see below). But the claims of the '288 patent make clear that the digital identification, while residing on the hardware key / access key, can also be stored on the authentication server. For example,

**117.** A system for controlling access to protected computer resources provided via an Internet Protocol network, the system comprising:

at least one authentication server having an associated database to store (I) identity data of at least one access server, (ii) a digital identification associated with at least one client computer device requesting access to said protected computer resources, and (iii) data associated with said protected computer resources;

said at least one client computer device having an associated access key, said digital identification being derived from said access key;

. . .

('288 patent, 45:1-13). Moreover, the '288 patent specification reads as follows: "The digital ID created by the biometric data

would be compared to the digital ID already stored in the transaction clearinghouse for authenticity" (*Id.*, 22:20-22).

The parties do not seem to be at odds on this point. Prism avows that "the claims and Specification [of the '288 patent] . . . state that digital identification may be stored in both a hardware key/access key and in a database associated with the authentication server" (Filing No. 124, at 30). Meanwhile, defendants state, "this portion of the ['288 patent] specification [22:20-22] teaches that the digital identification is stored on the hardware/access key as well as at the authentication server" (Filing No. 126, at 26). The Court notes that if the digital identification is not stored in two places, then a comparison cannot be made.

The Court agrees with Prism's assessment: "[T]he claims expressly recite the digital data [sic] being in a particular place, whether it's on the access key or on the database, so to put the location into the construction seems to be doubling up on what the claims expressly require" (*Markman* Hearing Transcript, at 113:2-6). The Court finds that defendants' construction of digital identification is redundant given the construction of hardware key / access key below and in light of the relevant claims that include the term being construed. The Court adopts the same construction as in the Delaware Case and in the Adobe Case: "**Digital identification**" is

construed to mean "**digital data whose value is known in advance or calculated at the moment.**"

**E. "Identity Data" terms**

Prism's Proposed Constructions	Defendants' Proposed Constructions
<p><b>"identity data":</b> "data sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources"</p>	<p><b>"identity data":</b> Defendants believe that the term "identity data" should be construed within the phrases in which it appears in the claims, not as a separate term, but in the event the Court determines "identity data" should be construed alone, the term should be construed as: "Data including digital identification sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources"</p>
<p><b>"identity data associated with at least one client computer device":</b> "data related to the client computer that is sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources"</p>	<p><b>"identity data associated with at least one client computer device":</b> "Data including digital identification, sufficient for the system to determine whether a client computer device is authentic and/or is entitled to access protected resources"</p>
<p><b>"identity data of at least one access server":</b> "data related to the access server that is sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources"</p>	<p><b>"identity data of at least one access server":</b> "data sufficient for the system to determine whether an access server is authentic and/or is entitled to access protected resources"</p>

The Delaware Court construed the term "identity data" as it relates to the subscriber client computer" in the '416 patent to mean "data sufficient for the patented system to determine whether a person, organization, and/or computer is authentic and/or is entitle[d] to a[cc]ess said selected computer resources" (Delaware Order at 3). In the Adobe Case, this Court construed the term "identity data" in the context of the '288 patent to mean "data sufficient for the system to determine whether a person, organization, and/or computer is authentic and/or is entitled to access protected resources," which is identical to Prism's current proposal (2012 Adobe Order, at 31).

The parties disagree as to the construction for the term "identity data" by itself, or, in the alternative, for the constructions of two phrases wherein "identity data" appears. Yet the parties are in agreement as to a third phrase in which "identity data" appears and have stipulated as follows: "**Identity data of a subscriber identity module associated with at least one client computer device**" is stipulated to mean "**data sufficient for the system to determine whether a subscriber identity module associated with at least one client computer device is authentic and/or is entitled to access protected resources**" (Schedule B, Filing No. 110). This stipulation essentially adopts this Court's construction of "identity data" from the Adobe Case and inserts it into the phrase to be construed. In light of this stipulation, the Court in this case will not construe the

individual phrase "identity data" again, but will construe the phrases in which it appears, consistent with the Adobe Case construction, having not been "otherwise compelled" to give the same claim term in the '288 patent a different construed meaning.

*Omega Eng'g*, 334 F.3d at 1334.

**1. "Identity data associated with at least one client computer device."** The parties' proposed constructions of this phrase differ in two ways. First, defendants propose that the phrase "including digital identification" be inserted into the construction.

Prism states, "Such a construction would render superfluous claim terms in the '288 patent that separately recite this limitation -- a violation of a bedrock principle canon of claim construction" (Filing No. 118, at 31). Prism continues, "For example, claims 1, 31, 62, and 87 of the '288 patent specifically recite identity data comprising 'digital identification.' By adding a 'digital identification' limitation to the term 'identity data', Defendants effectively render superfluous the term 'comprising said digital identification' . . ." (*Id.*, at 31 (internal citation omitted)).

Prism also states that "Defendants' proposed construction violates the doctrine of claim differentiation. When Prism wanted to draft claims that required digital identification, it did so. And when Prism [wanted to draft] claims that did not recite digital identification, it did so as

well" (*Id.*, at 32). "Prism sought and obtained claims with different scope and these differences should not be rendered meaningless" (*Id.*).

Defendants emphasize the fact that while the '288 patent claims "explicitly require that the identity data of the client computer device include a digital identification," the '345 and '155 patents do not share such a requirement (Filing No. 114, at 36). Defendants argue that the digital identification must be read back into the '345 and '155 patents due to Prism's disclaimer during the prosecution of the '288 patent. Specifically, defendants note Prism's statement to the USPTO in an attempt to distinguish a prior art reference ("Tabuki"):

In the Office Action, the Examiner rejected claims 1-8, 11, 12, 15, and 18 under 35 U.S.C. § 103(a) as being unpatentable over U.S. Patent No. 5,841,970 to Tabuki in view of U.S. Patent No. 6,377,994 to Ault et al. . . . The invention of applicant's claim 1 uses identity data that includes digital identification generated by a hardware key associated with the client computer device to identify the client computer device. In contrast, Tabuki's invention uses a pen tablet to capture and digitize the user's signature. This digitized signature is held in volatile memory in the tablet and is discarded once sent to the verification server. Therefore, the signature data of Tabuki is not digital identification generated by a hardware key associated with the client computer device to identify the client computer device as

recited in amended claim 1 of applicant's invention.

(Ex. 12, Filing No. 117, at 21-22).

Prism responds, "What the prosecution history actually shows is that Prism's distinction over the Tabuki reference focused on the differences between signature data described in Tabuki and the particular way the claimed digital identification was generated in the pending claim . . ." (Filing No. 124, at 34).

This argument focusing on Tabuki's use of a *pen tablet* to capture and digitize a *signature* as being different than the particularly claimed digital identification being generated by a hardware key in no way is a clear and unequivocal disclaimer that identity data can only come from an external hardware key, as argued by Defendants.

(*Id.*, at 35). The Court agrees with Prism that its statement to the USPTO does not clearly and unequivocally disavow an invention that does not include a digital identification.

The second difference in the proposed constructions has to do with the location of the identity data. Prism's proposed construction translates "associated with" as "related to." Defendants' proposed construction more faithfully follows the construction of "identity data" by itself, with the more specific "client computer device" replacing "a person, organization, and/or computer." The Court finds that defendants' substitution is a straightforward application of the previous construction

relative to the claim language being construed with this phrase, and the Court adopts this aspect of defendants' construction.

The Court construes "**identity data associated with at least one client computer device**" to mean "**data sufficient for the system to determine whether a client computer device is authentic and/or is entitled to access protected resources.**"

**2. "Identity data of at least one access server."**

Prism's proposed construction translates "of" as "related to." Again, defendants' proposed construction more faithfully follows the construction of "identity data" by itself, with the more specific "access server" replacing "a person, organization, and/or computer." The Court construes "**identity data of at least one access server**" to mean "**data sufficient for the system to determine whether an access server is authentic and/or is entitled to access protected resources.**"

**F. "hardware key / access key" (and "external")**

Prism's Proposed Construction:	Defendants' Proposed Construction:
"An external hardware device or object from which the predetermined digital identification can be read"	"An external hardware device or external object from which the predetermined digital identification can be read"

The Delaware Court construed "hardware key" to mean "an external hardware device or object from which the predetermined digital identification can be read," and this Court gave the same construction to both "hardware key" and "access key" in the Adobe

Case. Defendants now wish to add another instance of "external" before the word "object," asking the Court to verify that the word "external" in the Adobe Case construction modifies both "hardware device" and "object."

**1. "Shared Object 66."** At oral argument, Prism admitted that there was "[n]o dispute that external modifies object and external hardware device from Court's prior construction" (Prism Slide 38; see *Markman Hearing Transcript*, at 116:24-117:6). But Prism's understanding of the word "object" bears scrutiny. Prism emphasizes the presence of a "shared object **66**" in the '288 patent specification, where the "object" is software (Filing No. 118, at 23). For example, "The server shared object **66** is a binary module which provides function pointers to a web server **69** to perform secure transaction server **34** specific operations" ('288 patent, 7:59-61). Prism claims that a person having ordinary skill in the art would then understand that the "object" in the hardware key construction could be software as well (Filing No. 118, at 23).

Defendants disagree: "Although ['288 patent, 7:59-61] mentions an 'object' that is software, the passage refers to the secure transaction system of the invention, which has nothing to do with the hardware key/access key associated with the client computer device. The specification never describes internal software as the hardware key/access key" (Filing No. 126, at 17).

As defendants point out, the '288 patent specification describes the hardware key as follows:

In accordance with another important aspect of the present invention, and referring to FIG. 21, a hardware token access device 450 for use as the hardware key 54 is shown in the illustrated functional block diagram. The access device 450 is an external hardware device, such as the iKey 1000 USB Smart Token device manufactured by Rainbow Technologies of Irvine, Calif. The hardware token access device 450 preferably connects to the USB port of the account holder's personal computer. The major function of the hardware token access device 450 is to uniquely identify a [sic] account holder that desires to access the transaction services and computer resources of an untrusted network, such as the Internet. It is used in conjunction with the username, password, and/or PIN to provide two factor authentication. Generally, two factor authentication provides that something is known (e.g., the username and password) and something is held (e.g., the physical hardware token that is attached to the computer or built into the computer). While the Rainbow iKey 1000 USB Smart Token is the preferred embodiment for the hardware token access device 450, it should be understood that the two factor authentication could be provided by some other physical device, such as a credit card, a key, an ATM card, or the like which is known to have been assigned and given to a specific person.

('288 patent, 19:30-53).

The Court does not doubt that a person skilled in the art would read "shared object **66**" as referring to software. But was that the understanding of the word "object" by the Delaware Court at the time of its construction of hardware key, or was "object" taken as a synonym of or variant on "device?" After all, if the "object" in the construction were taken to mean "software," it would lead to the anomalous result that a "hardware key" could be construed as "software from which the predetermined digital identification can be read," reading out the "hardware" limitation of "hardware key" entirely.

An examination of the Delaware Memorandum answers the question. In its brief, Prism pointed out to the Delaware Court that "[t]he '416 patent specifically teaches that the hardware key may be attached to and separable from the user's computer, or it may be built in to the computer" (Ex. 5, Filing No. 116, at 34). The Delaware Court rejected this contention:

After reviewing the term "hardware key" in the context of the specification, the Court concludes that the specification requires that the hardware key be an external hardware device. The Court declines to adopt Plaintiff's proposal that the key can be built into the computer, because the 'major function of the [hardware key] is to uniquely identify a user,' and the specification teaches that the key should be something 'which is known to have been assigned and given to a specific person.' A hardware key built in to a computer is

computer-specific, not user-specific.

*Prism*, 512 F. Supp. 2d at 188 (internal citations and footnote omitted).

The Delaware Court does not explain why it added the words “or object” to the construction.<sup>9</sup> Moreover, *Prism* did not alert the Delaware Court to the ostensible difference between the terms “device” and “object” in its opening brief. But given the Delaware Court’s interpretation of “hardware key” above, this Court cannot imagine that by adding the word “object,” the Delaware Court would negate its clear statement that “the specification requires that the hardware key be an external hardware device.” And without a doubt, in this Court’s adoption of the Delaware Court’s construction in the *Adobe* Case, this Court intended only the usual and everyday meaning of the word “object,” and not the context of software.

**2. External Object.** During the *Adobe* Case construction of hardware key, the phrase “external hardware device or object” was not in dispute. Defendants state, “[I]n *Adobe*, *Prism* did not dispute that the access key must be external. *Prism* should not now be allowed to take a position inconsistent with the one it took in *Adobe*” (Filing No. 126, at 17 (internal citation and footnote omitted)). The Court finds,

---

<sup>9</sup> *Prism*’s proposed construction for hardware key was “a device or object from which data may be read or emitted” (Ex. 5, Filing No. 116, at 33).

as it intended from the beginning, that the word "external" also modifies the word "object," as Prism itself now admits.

Defendants originally proposed that "external" be construed as "physically located outside of and physically attached to and detachable from," a narrow definition that would negate the Delaware Court's conclusion that the hardware key need not be physically attached:

Though the invention's preferred embodiment involves a hardware key that is physically attached to the subscriber client computer via a port interface, the specification also lists acceptable alternatives to the preferred embodiment which need not be physically attached, including "a credit card, a key, an ATM card, or the like which is known to have been assigned and given to a specific person." Therefore, the Court finds that the specification anticipates hardware keys which are not physically attached.

*Prism*, 512 F. Supp. 2d at 188-89 (quoting '416 patent, 22:1-5).

The parties have now stipulated that the word "external" should be given its plain and ordinary meaning. Yet Prism claims that the "plain and ordinary meaning" of "external" is "separate from" (Filing No. 118, at 21). While defendants' original proposed construction was too narrow, the Court finds that Prism's definition is too broad, and is not, in fact, the plain and ordinary meaning of the term. Webster's New College Dictionary defines "external," as relevant here, as follows: "relating to, existing on, or connected with the outside or an

outer part." *Webster's New College Dictionary Third Edition* 405 (Houghton Mifflin Harcourt Publishing Company 2008). Similarly, the New Oxford American Dictionary defines "external," as relevant here, as follows: "belonging to or forming the outer surface or structure of something." *New Oxford American Dictionary Third Edition* 613 (Oxford University Press 2010). Both definitions are more narrow than Prism's "separate from," because they contain the concept of "outside" or "outer."

The Federal Circuit advises a district court to act under these circumstances, so as to avoid requiring a jury to construe a term in violation of *Markman*:

A determination that a claim term "needs no construction" or has the "plain and ordinary meaning" may be inadequate when a term has more than one "ordinary" meaning or when reliance on a term's "ordinary" meaning does not resolve the parties' dispute. In this case, for example, the parties agreed that "only if" has a common meaning, but then proceeded to dispute the scope of that claim term, each party providing an argument identifying the alleged circumstances when the requirement specified by the claim term must be satisfied (e.g., at all times or during steady state operation). In this case, the "ordinary" meaning of a term does not resolve the parties' dispute, and claim construction requires the court to determine what claim scope is appropriate in the context of the patents-in-suit. This court has construed other "ordinary" words

for these and other related reasons. . . .

When the district court failed to adjudicate the parties' dispute regarding the proper scope of "only if," the parties presented their arguments to the jury. By failing to construe this term, the district court left the jury free to consider these arguments.

*O2 Micro*, 521 F.3d at 1361-62. Consequently, the Court will provide a construction for the term "external."

The Court's search of the '288 patent for the word "external" indicates that the term does not appear in the claims. The term does appear in the claims of the '345 patent and the '155 patent, however, in the context of an "external device" or an "external object" (See '345 patent, claims 6, 7, 10, 54, 55, and 58; '155 patent, claims 4, 5, 6, 7, 41, 42, 43, and 44).

The Court's search also indicates that the term appears in the specification in the quote above ('288 patent, 19:30-53), plus one other: "A read/write control logic block **484** manages all the internal and external transfer of data controlled status, while a control register **486** initializes the functional configuration of the access device **450**" (*Id.*, 19:65-20:2). Also relevant is the Delaware Memorandum, which, as quoted above, clearly uses the term "external" to oppose the concept of "built in to the computer."

After consideration of the claims themselves, the specification, the Delaware Memorandum, and appropriate extrinsic

evidence, the Court construes the term "**external**" to mean: "**relating to, existing on, or connected with the outside or an outer part.**"

In summary, in this Court's construction of the term "hardware key," the word "external," as construed here, modifies each of the terms "hardware device" and "object." The Court construes "**hardware key**" and "**access key**" each to mean "**an external hardware device or external object from which the predetermined digital identification can be read,**" with the understanding that this construction is only meant to clarify, but not augment, previous constructions of the same terms.

#### G. "**authorization level(s)**"

Prism's Proposed Construction:	Defendants' Proposed Construction:
Prism argues that no construction is required and that the term should be given its plain and ordinary meaning.	"A value identifying particular protected computer resources that are authorized by the access server to be received by the client computer device"

``[I]f we once begin to include elements not mentioned in the claim, in order to limit such claim . . . , we should never know where to stop.'' *Phillips*, 415 F.3d at 1312 (quoting *McCarty v. Lehigh Valley R.R. Co.*, 160 U.S. 110, 116 (1895)).

The term "authorization level" was not construed in either the Delaware Case or the Adobe Case. But the related term "authorizing" was construed to mean "determining whether to grant

access to," as stipulated by the parties in the Adobe Case, and it is also so stipulated here.

Prism cites dependent claim 39 of the '345 patent:

**39.** The method of claim 1, further comprising assigning one of a plurality of authorization levels to the at least a portion of the protected computer resources, assigning a particular authorization level to the identity data associated with the at least one client computer device, and only permitting access to particular protected computer resources by the at least one client computer device permitted by the particular authorization level.

('345 patent, 36:36-43). Prism states: "There is no dispute as to the meaning of 'authorization,' i.e. 'determining whether to grant access to.' Similarly, 'levels' has a well understood plain and ordinary meaning in this context -- i.e., differing degrees. Accordingly, no particular construction is warranted for 'authorization levels' beyond its plain and ordinary meaning" (Filing No. 118, at 41). Prism specifically objects to defendants' proposed construction because it "improperly imports two limitations to the term" (*Id.*, at 41).

The Court agrees that defendants' proposed construction inappropriately limits the term "authorization level(s)." The parties have stipulated to the construction of the terms "authorize" and "authorizing," and the Court finds that the term "level(s)" should be given its plain and ordinary meaning.

Consequently, the Court will not provide a construction for the term "authorization level(s)." Accordingly,

IT IS ORDERED: For the purposes of United States Patent Nos. 7,290,288, 8,127,345, and 8,387,155,

1) As jointly stipulated by the parties (Schedule B, Filing No. 110), the following terms are construed as indicated:

- a. "**Access server**" is construed to mean "**server software that makes available information or other resources.**"
- b. "**Adapted to forward**" / "**adapted to forward . . . said identity data . . .**" is construed to mean "**configured to forward**" / "**configured to forward . . . identity data.**"
- c. "**Adapted to selectively require**" is construed to mean "**configured to choose to require.**"
- d. "**Authenticate**" / "**authenticating**" is construed to mean "**determine/determining that something is, in fact, what it purports to be.**"
- e. "**Authentication server**" is construed to mean "**server software that is independent of the access server and is capable of storing data and controlling access to protected computer resources of the access server.**"
- f. "**Authorize** / "**authorizing**" is construed to mean "**determine / determining whether to grant access to.**"
- g. "**Deriving**" / "**derived**" is construed to mean "**calculating / calculated from a source.**"
- h. "**Generating**" / "**generate[d]**" is construed to mean "**bringing / bring / brought into existence.**"
- I. "**Identity data of a subscriber identity module associated with at least one client computer device**" is construed to mean "**data sufficient for the system to determine whether a subscriber**

**identity module associated with at least one client computer device is authentic and/or is entitled to access protected resources."**

- j. "**Selectively requiring. . . [said/the] client computer device to forward**" is construed to mean "**choosing to require that the client computer device transmit certain information.**"
  - k. "**Server computer**" is construed to mean "**a computer that makes available information or other resources.**"
  - l. "**One of derived and generated**" is construed to mean "**calculated from a source or brought/bringing into existence.**"
- 2) As jointly stipulated by the parties (Schedule B, Filing No. 110), **the preambles of the asserted claims are limiting.**
- 3) The Court construes disputed terms as follows:
- a. The "**Internet Protocol network**" terms ("**an Internet Protocol network,**" "**network utilizing at least one Internet Protocol,**" and "**a network utilizing at least one Internet Protocol**") are each construed to mean "**an untrusted network using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, HTTP, and HTTP/IP, where untrusted is defined as a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous.**"
  - b. "**Forward**" is construed to mean "**transmit.**" The Court will not construe the word "**receive**" and will give it its plain and ordinary meaning.
  - c. The "**protected computer resources**" terms ("**protected computer resources,**" "**protected resources,**" and "**protected resources of at least one server computer**") are construed to mean "**computer services, applications, or content that is stored within the secure transaction system**

**that can only be accessed by a server within the secure transaction system."**

- d. "**Digital identification**" is construed to mean "**digital data whose value is known in advance or calculated at the moment.**"
- e. "**Identity data associated with at least one client computer device**" is construed to mean "**data sufficient for the system to determine whether a client computer device is authentic and/or is entitled to access protected resources.**"  
  
"**Identity data of at least one access server**" is construed to mean "**data sufficient for the system to determine whether an access server is authentic and/or is entitled to access protected resources.**"
- f. "**Hardware key**" and "**access key**" are each construed to mean "**an external hardware device or external object from which the predetermined digital identification can be read,**" with the understanding that this construction is only meant to clarify, but not augment, previous constructions of the same terms.  
  
"**External**" is construed to mean: "**relating to, existing on, or connected with the outside or an outer part.**"

4) The Court will not provide a construction for the term "authorization level(s)."

DATED this 30th day of July, 2013.

BY THE COURT:

/s/ Lyle E. Strom

---

LYLE E. STROM, Senior Judge  
United States District Court

IN THE UNITED STATES DISTRICT COURT FOR THE  
DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV122
	)	
v.	)	
	)	
AT&T MOBILITY, LLC,	)	MEMORANDUM AND ORDER
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV123
	)	
v.	)	
	)	
SPRINT SPECTRUM L.P.,	)	
d/b/a SPRINT PCS,	)	
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV124
	)	
v.	)	
	)	
T-MOBILE USA, INC.,	)	
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV125
	)	
v.	)	
	)	
UNITED STATES CELLULAR	)	
CORPORATION, d/b/a U.S.	)	
CELLULAR,	)	
	)	
Defendant.	)	
	)	

PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV126
	)	
v.	)	
	)	
CELLCO PARTNERSHIP d/b/a	)	
VERIZON WIRELESS,	)	
	)	
Defendant.	)	
	)	

---

This matter is before the Court on the common *Daubert* motions (Filing No. 255 in 8:12CV122; Filing No. 216 in 8:12CV123; Filing No. 229 in 8:12CV124; Filing No. 209 in 8:12CV125; Filing No. 199 in 8:12CV126)<sup>1</sup> of the five defendants in five separate cases. Pursuant to Section 299 of Title 35, plaintiff Prism Technologies, L.L.C. ("Prism") opted to file separate actions against common alleged infringers of its patents (35 U.S.C. § 299(a), (b); Filing No. 135). In the interest of judicial economy, the parties agreed to allow the filing of "common motions for summary judgment" and "common *Daubert* motions" by the Defendants, AT&T Mobility L.L.C., Sprint Spectrum L.P., T-Mobile U.S.A., Inc., United States Cellular Corporation d/b/a U.S. Cellular, and Cellco Partnership d/b/a Verizon Wireless (referred to heretofore as the "defendants") (Filing No.

---

<sup>1</sup> For ease of citation, the Court will refer to the filings in the AT&T Mobility L.L.C. case (8:12CV122).

226). The defendants filed the current common *Daubert* motion to exclude the opinions and testimony of John Minor ("Minor"). The matter has been fully briefed and is ready for disposition (Filing No. 259, Filing No. 334, Filing No. 365). After review of the motion, briefs, indices of evidence, and relevant case law, the Court finds as follows.

## **I. BACKGROUND**

Originally, Prism alleged infringement of three asserted patents (Filing No. 1). Ultimately, Prism narrowed the scope of this action to two patents: U.S. Patent No. 8,127,345 ("Patent '345") and U.S. Patent No. 8,387,155 ("Patent '155") (Filing No. 1; Filing No. 242, 9; Filing No. 243-4, 3; Filing No. 243-5, 2). Prism dropped its third asserted patent, U.S. Patent 7,290,288 ("Patent '288"), from this action (*Id.*).

The United States Patent and Trademark Office ("PTO") issued Patent '345, entitled "METHOD AND SYSTEM FOR MANAGING ACCESS TO PROTECTED COMPUTER RESOURCES VIA AN INTERNET PROTOCOL NETWORK," on February 28, 2012, from an application filed October 30, 2007 (Filing No. 1-6, at 1). Patent '345 is allegedly a continuation of Patent '288, entitled "METHOD AND SYSTEM FOR CONTROLLING ACCESS, BY AN AUTHENTICATION SERVER, TO PROTECTED COMPUTER RESOURCES PROVIDED VIA AN INTERNET PROTOCOL NETWORK" and filed on August 29, 2002 (*Id.*).

The PTO issued Patent '155, entitled "SYSTEM FOR MANAGING ACCESS TO PROTECTED COMPUTER RESOURCES," on February 26, 2013, from an application filed November 11, 2010, with the PTO. Prism contends that the Patent '155 application was a continuation of the Patent '345 application.

Prism has a fourth, unasserted patent, U.S. Patent No. 6,516,416 ("'416 Patent"), entitled "SUBSCRIPTION ACCESS SYSTEM FOR USE WITH AN UNTRUSTED NETWORK." The Court has referenced this patent in its prior orders (*E.g.*, Filing No. 132).

B. PROCEDURE

On April 4, 2012, Prism filed its complaints against AT&T and various other cellular phone providers in separate actions, alleging direct infringement, indirect contributory infringement, and indirect inducement of infringement of Patents '345 and '155 (Filing No. 1, 85). The complaint was amended September 21, 2012 (Filing No. 40) and March 1, 2013 (Filing No. 85). On April 23, 2013, the parties submitted a Joint Claim Construction Statement and the Court conducted a *Markman* hearing on July 2, 2013 (Filing Nos. 110, 130). The Court issued its *Markman* order on July 30, 2013, accepting jointly stipulated terms and construing disputed terms (Filing No. 132).

An integral construction in the *Markman* order was the term "Internet Protocol Network" (hereinafter "IPN"), which

appears ubiquitously in the asserted claims (Patent '345 claim Nos. 1, 50; Patent '155 claim Nos. 50, 56, 74). The Court construed IPN to mean "**an untrusted network using any protocol of the Internet Protocol Suite including at least one of IP, TCP/IP, UDP/IP, HTTP, and HTTP/IP . . .**" (Filing No. 132, at 12-30). The Court further defined "**untrusted**" as "**a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous.**" (*Id.*).

Prism has retained experts to testify and offer testimony and opinions at trial regarding damages and the systems in this case. The parties submitted their briefs and a *Daubert* hearing was held August 27, 2014. Minor will offer the following, paraphrased, expert opinions at trial:

1. The cost for the defendants to build a backhaul<sup>2</sup> is two to five times more than each defendant spends on leasing a backhaul.
2. The Court's *Markman* order construes IPN to mean in part "**a public network with no single controlling organization.**"
3. The defendants' backhauls constitute IPNs.

---

<sup>2</sup> The backhaul is a physical infrastructure which the defendant does not own but rather leases from third parties under strict contractual terms.

The defendants first move to exclude those sections within Minor's report where he estimates the costs of the backhaul. The defendants then move to exclude Minor's testimony regarding his interpretation of Internet Protocol Network and whether the defendants' backhaul constitute the Internet Protocol Networks.

## **II. STANDARD OF REVIEW**

This Court must determine whether Minor's specialized knowledge will assist the trier of fact to understand evidence or to determine a fact in issue. Fed. R. Evid. 702. Under Rule 702, the Court must consider whether (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness has applied the principles and methods reliably to the facts of the case. The Court's role is to act as a gatekeeper, excluding evidence if it is based upon unreliable principles or methods, or legally insufficient facts and data and must be sufficiently tied to the facts of the case that it will aid the jury in resolving a factual dispute. *Daubert*, 509 U.S. at 595.

The Court is mindful not to overstep its gatekeeping role and weigh facts, evaluate the correctness of conclusions, impose its own preferred methodology, or judge credibility, including the credibility of one expert over another. *Apple, Inc. v. Motorola, Inc.*, 757 F.3d 1286, 1314 (Fed. Cir. 2014)

(citing *Smith v. Ford Motor Co.*, 215 F.3d 713, 718 (7th Cir. 2000). These tasks are solely reserved for the fact finder. *Id.* citing *Smith*, 215 F.3d at 718. The proponent of the expert testimony must prove its admissibility by a preponderance of the evidence. *Daubert*, 509 U.S. at 592-93, n.10.

### **III. DISCUSSION**

The defendants' arguments against Minor's opinion and testimony is two fold. First, the defendants object to the sufficiency of the evidence upon which Minor relied to establish the basis of his estimations. Filing No. 334, at 6-7. Second, the defendants argue that Minor deliberately modified the term IPN, disregarding the Court's *Markman* order. *Id.*

#### A. SUFFICIENCY

Minor has experience creating and leasing backhaul systems. The defendants primarily object to the fact that his experience is not specifically in creating and leasing backhaul systems in the cellular industry. Filing No. 634, at 8. The Court finds that Minor's experience is sufficiently specific to the facts in this case to allow Minor to rely upon his experience. The Court also finds the distinction between "cellular backhauls" and "other backhauls" does not invalidate Minor's experience as it relates to this case. This argument is best made in cross examination.

The Court also finds Minor reasonably relied upon quantitative analyses. To the extent these reports fail to incorporate specific issues for the defendants, the defendants may bring that issue to the jury's attention at trial.

Finally, the defendants raise an interesting issue as to whether Prism is shifting its burden from its damages expert to its technical expert in order to circumvent the scientific requirements of calculating damages. Though Minor's opinion is the integral piece of Prism's damages model, the Court will exclude Prism's damages model in its entirety, so the Court will not address this final issue.

B. *MARKMAN*

Below is a visualization of the parties' argument regarding the interpretation of untrusted:

Minor's interpretation	The Court's <i>Markman</i> order
<b>"a public network with no single controlling organization, with the path to access the network being undefined and the user being anonymous."</b>	<b>"a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous."</b>

The effect of this distinction is significant and potentially dispositive. If Minor's reading is correct, only a single

organization may “control” a network in order to constitute a trusted network. Prism argues, because the defendants share control with multiple other organizations, there is no single controlling organization and the defendants’ networks are untrusted and therefore infringe.

If Minor is incorrect, one or more organizations may “control” a network. Any controlling organization in a public network, whether singular or plural, is not an untrusted network and the defendants’ networks, therefore, are trusted and do not infringe.

The parties concur on two issues. First, control exists at every level of the defendants’ networks. Second, the internet is the preferred embodiment of the Asserted Patents. The Court is mindful that experts are permitted to reasonably disagree as to the interpretation and application of the Court’s *Markman* order. However, they must not “cross[] the line by asserting claim constructions that are contrary to the court’s [construction].” *Transamerica Life Ins. Co. v. Lincoln Nat'l Life Ins. Co.*, 597 F. Supp. 2d 897, 910 (N.D. Iowa 2009) (citing *Kemin Foods, L.C. v. Pigmentos Vegetales Del Centro S.A. de C.V.*, 4:02CV40327, 2004 WL 5508752, \*4 (S.D. Iowa Sept. 9, 2004)). The issue is whether Minor’s interpretation of the *Markman* order is inapposite or merely germane to the order.

Minor interpreted the *Markman* order in light of the "internet," the preferred embodiment of untrusted network in the Asserted Patents. Filing No. 334, at 23. The internet, according to Minor, is a "network-of-networks with many of the individual constituent components privately owned and controlled, but in the aggregate there is no controlling organization." Prism argues that because the defendants do not solely own all the portions of their networks, those networks constitute the internet -- an untrusted network. If the defendants purchases all the leased backhaul, then their networks would be trusted and not the internet.

First, the Court disregards Prism's argument that the defendants' experts have adopted Minor's interpretation. It is merely an ostensible misconstruction of the experts' testimony. See Filing No. 334, at 25 (focusing solely on "no one organization" but ignoring "or organizations").

Prism's primary argument is that the defendants' verbatim interpretation of the *Markman* order excludes the "internet." *Id.* at 24-26. The parties agree that the connection of all networks in the world is the public, uncontrolled, undefined pathway, anonymous-user aggregated internet. The parties agree portions of the aggregate internet may be controlled, but no single organization controls all of the

aggregate internet. The question is whether the defendants' networks, over which each exert an arguable level of control, can likewise constitute a public, uncontrolled, undefined pathway, anonymous-user internet like the aggregated internet. When does an organization exert sufficient control over its network in order for it to be trusted? This is a question of fact and the Court will not determine whether the defendants' networks exert sufficient control over the backhaul. The Court finds Minor's interpretation of the control element of untrusted does not stand inapposite of the *Markman* hearing and he may rely upon it at trial.

IT IS ORDERED that the defendants' motions (Filing No. 255 in 8:12CV122; Filing No. 216 in 8:12CV123; Filing No. 229 in 8:12CV124; Filing No. 209 in 8:12CV125; Filing No. 199 in 8:12CV126) are denied.

DATED this 29th day of September, 2014.

BY THE COURT:

/s/ Lyle E. Strom

LYLE E. STROM, Senior Judge  
United States District Court

IN THE UNITED STATES DISTRICT COURT FOR THE  
DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV123
	)	
v.	)	
	)	
SPRINT SPECTRUM L.P.,	)	
d/b/a SPRINT PCS,	)	
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV124
	)	
v.	)	
	)	
T-MOBILE USA, INC.,	)	
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV125
	)	
v.	)	
	)	
UNITED STATES CELLULAR	)	
CORPORATION, d/b/a U.S.	)	
CELLULAR,	)	
	)	
Defendant.	)	
	)	
PRISM TECHNOLOGIES LLC,	)	
	)	
Plaintiff,	)	8:12CV126
	)	
v.	)	
	)	
CELLCO PARTNERSHIP d/b/a	)	ORDER
VERIZON WIRELESS,	)	
	)	
Defendant.	)	
	)	

This matter comes before the Court on common *Daubert* motions filed by defendants Sprint Spectrum ("Sprint"), T-Mobile U.S.A. ("T-Mobile"), United States Cellular Corp. ("U.S. Cellular"), and Cellco Partnership ("Cellco") (collectively, the "Carrier Defendants") in four related cases. In their motions (Filing No. 336 in 8:12CV123; Filing No. 290 in 8:12CV124; Filing No. 279 in 8:12CV125; and Filing No. 261 in 8:12CV126), defendants seek to exclude the expert opinion and testimony of Mr. Malackowski.<sup>1</sup> The Court granted the Carrier Defendants' request for oral arguments and arguments were held May 20, 2015.

#### I. BACKGROUND

Prism accuses the Carrier Defendants of infringing upon its patents, 8,127,345 ("the '345 Patent") and 8,287,155 ("the '155 Patent"). Though Prism filed different actions against each Carrier Defendant, the parties agreed to common resolution of certain issues which affected all the cases. For example, Prism, AT&T Mobility, and the remaining Carrier Defendants agreed to resolve "common" issues in summary judgment and *Daubert* motions in addition to case specific issues. Filing No. 214. The Court adopted this policy and resolved the common issues pertaining to

---

<sup>1</sup> The briefs of the parties are substantially identical in the four cases and the Court will cite to docket number 8:12CV123 throughout the remainder of this opinion.

Prism's expert witnesses and various legal issues. The Court made a determination in the matter of *Prism Technologies LLC v. AT&T Mobility, LLC* (Docket No. 8:12CV122) (the "AT&T Matter") which plays into the Carrier Defendants' current motions. The Court granted the Carrier Defendants' motions to exclude the expert report and opinions of Mr. Malackowski, Prism's damages expert, due to the method of his damages calculations. Filing No. 246. Following the AT&T Matter, the Court granted Prism leave to amend the reports of its damages and validity experts based on agreements executed by Prism and AT&T Mobility, L.L.C. ("AT&T") that resolved the AT&T Matter.<sup>2</sup>

Mr. Malackowski has offered three damages theories. The first was excluded. The second and third theories were introduced in his amended report. The Court finds the following illustration instructive in distinguishing the major differences between the theories:

---

<sup>2</sup> Though a major issue in their briefs, the parties stated at oral arguments that Prism will not use the confidential figures from the AT&T Matter in the present and successive Carrier Defendant Matters. Therefore, the Court considers the matter withdrawn and moot.

	<b>First Theory- Revenue</b>	<b>Second Theory - Cost-Savings (I)</b>	<b>Third Theory - Cost-Savings (II)</b>
<b>Starting Point</b>	Total Service Revenues (Voice + Data)	Alleged Cost Savings (Voice + Data)	Alleged Cost Savings (Voice + Data)
<b>Distinction Between Voice and Data Services</b>	Limited to Data Revenues	No Limitation (Voice + Data Included)	Limit to Alleged Data-Related Cost Savings
<b>Apportionment Metric</b>	<b>12.1% (87.9% Reduction)</b>	-- <b>(No Reduction)</b>	-- <b>(No Reduction)</b>
<b>Royalty Base</b>	X	Y	Z
<b>Royalty Rate</b>	<b>3.5%</b>	<b>3.5%</b>	<b>3.5%</b>
<b>Royalty</b>	<b>.035X</b>	<b>.035Y</b>	<b>.035Z</b>

(See Carrier Defendants' Slide No. 3 for Malackowski *Daubert Hearing*).

## II. LEGAL STANDARDS

The Court must determine whether Mr. Malackowski's specialized knowledge will assist the trier of fact to understand evidence or to determine a fact at issue. Fed. R. Evid. 702. Under Rule 702, the Court must consider whether (1) the testimony is based upon sufficient facts or data, (2) the testimony is the product of reliable principles and methods, and (3) the witness

has applied the principles and methods reliably to the facts of the case.

Royalty damage calculations are governed by case law:

Upon a showing of infringement, a patentee is entitled to "damages adequate to compensate for the infringement, but in no event less than a reasonable royalty for the use made of the invention by the infringer." 35 U.S.C. § 284. A "reasonable royalty" derives from a hypothetical negotiation between the patentee and the infringer when the infringement began. See, e.g., *Unisplay, S.A. v. Am. Elec. Sign Co.*, 69 F.3d 512, 517 (Fed. Cir. 1995). A comprehensive (but unprioritized and often overlapping) list of relevant factors for a reasonable royalty calculation appears in *Georgia-Pacific Corp. v. United States Plywood Corp.*, 318 F. Supp. 1116, 1120 (S.D.N.Y. 1970).

Thus, the trial court must carefully tie proof of damages to the claimed invention's footprint in the market place. See, e.g., *Grain Processing Corp. v. Am. Maize-Prod. Co.*, 185 F.3d 1341, 1350 (Fed. Cir. 1999) ("To prevent the hypothetical from lapsing into pure speculation, this court requires sound economic proof of the nature of the market and likely outcomes with infringement factored out of the economic picture."); *Riles v. Shell Exploration & Prod. Co.*, 298 F.3d 1302, 1312 (Fed. Cir. 2002) ("[T]he market would pay [the patentee] only for his product

. . . . [The patentee's damages] model [does not support the award because it] does not associate [the] proposed royalty with the value of the patented method at all, but with the unrelated cost of the entire Spirit platform."). Any evidence unrelated to the claimed invention does not support compensation for infringement but punishes beyond the reach of the statute.

*ResQNet.com, Inc. v. Lansa, Inc.*, 594 F.3d 860, 868-69 (Fed. Cir. 2010). "A damages theory must be based on 'sound economic and factual predicates.'" *LaserDynamics, Inc.*, 694 F.3d at 67 (citing *Riles v. Shell Exploration & Pro. Co.*, 298 F.3d 1302, 1311 (Fed. Cir. 2002)).

The proponent of the expert testimony must prove its admissibility by a preponderance of the evidence. *Daubert*, 509 U.S. at 592-93, n.10. "[T]estimony is inadmissible if it is speculative, unsupported by sufficient facts, or contrary to the facts of the case." *Marmo v. Tyson Fresh Meats, Inc.*, 457 F.3d 748, 757 (8th Cir. 2006). "When the analytical gap between the data and proffered opinion is too great, the opinion must be excluded." *General Elec. Co. v. Joiner*, 522 U.S. 136, 146 (1997).

The Carrier Defendants object to the Second and Third theories on various grounds. After review of the filings, oral arguments and relevant case law, the Court will deny the Carrier Defendants' motions. Accordingly,

IT IS ORDERED:

1) In Case Number 8:12CV123, the defendant's motion (Filing No. 336) to exclude the testimony of Mr. Malackowski is denied.

2) In Case Number 8:12CV124, the defendant's motion (Filing No. 290) to exclude the testimony of Mr. Malackowski is denied.

3) In Case Number 8:12CV125, the defendant's motion (Filing No. 279) to exclude the testimony of Mr. Malackowski is denied.

4) In Case Number 8:12CV126, the defendant's motion (Filing No. 261) to exclude the testimony of Mr. Malackowski is denied.

DATED this 8th day of June, 2015.

BY THE COURT:

/s/ Lyle E. Strom

---

LYLE E. STROM, Senior Judge  
United States District Court

IN THE UNITED STATES DISTRICT COURT

FOR THE DISTRICT OF NEBRASKA

PRISM TECHNOLOGIES, LLC,	)	
	)	
Plaintiff,	)	8:12CV123
	)	
v.	)	
	)	
SPRINT SPECTRUM L.P., D/B/A	)	MEMORANDUM AND ORDER
SPRINT PCS,	)	
	)	
Defendant.	)	
	)	

---

This matter is before the Court on cross motions *in limine* from both the plaintiff Prism Technologies, L.L.C. ("Prism") (Filing No. [357](#)) and defendant Sprint Spectrum, doing business as Sprint PCS ("Sprint") (Filing No. [361](#), Filing No. [362](#), Filing No. [363](#)). After review of the motions, briefs, indices of evidence, and relevant case law,

IT IS ORDERED:

I. PRISM'S MOTIONS *IN LIMINE*

1) Neither party may refer to Prism's prior patent infringement lawsuits or current affiliated entities and their current business or litigation activities, except that the parties may discuss Prism's settlement agreements to establish reasonable damages.

Deferred until trial.

2) Sprint may not argue that Prism failed to test Sprint's systems.

Granted as to Sprint's systems.

3) Neither party may refer to whether testimony from any expert witness was excluded in a prior case.

Granted.

4) Neither party may present testimony from prospective damages experts concerning whether the other party's expert complied with applicable law. This does not exclude the experts from providing testimony regarding the legal standard applied.

Denied.

5) Sprint may not argue that it respects the intellectual property rights of others and Prism will not refer to the fact that Sprint is often sued for and settles patent infringement lawsuits.

Deferred until trial.

8)<sup>1</sup>) Sprint may not present evidence or argument that Mr. Minor has served as an expert for individuals accused of sexual assault. The parties may note that Mr. Minor has served as an expert for the prosecution and defense in capital murder cases and in civil actions.

Granted.

10) Sprint may not present argument that multiple GSM documents are anticipatory references.

Denied.

11) The parties may not rely on transcripts from the trial testimony of the parties' experts or AT&T's fact witnesses from the trial in the matter of Prism Techs., LLC v. AT&T Mobility, LLC, (8:12CV122).

---

<sup>1</sup> Prism originally asserted twenty-one motions but later resolved six of those motions. Compare Filing No. 358, at 2-3, with Filing No. 378 (withdrawing motions *in limine* 6, 7, 9, 20), and Filing No. 379 (same), and Filing No. 392 (withdrawing motions *in limine* 13 and 14), and Filing No. 393 (same). This opinion uses the original enumeration of the motions in Filing No. 357 and related filings.

Denied. Parties may use the prior testimony of an expert witness from the AT&T trial to cross-examine the same witness in this trial.

12) The parties may not rely on deposition transcripts of Prism's expert witnesses from the matter of Prism Techs., LLC v. AT&T Mobility, LLC, 8:12CV122 (D. Neb.).

Denied. Parties may use the prior testimony of an expert witness from depositions in the AT&T matter to cross-examine the same witness in this trial.

15) Sprint's expert, Scott D. Hampton, may not rely on technical documents contained in Exhibit K to his expert report that were not disclosed during fact discovery or cited in the reports of Sprint's technical expert.

Denied.

16) Sprint's expert, Scott D. Hampton, may not present trial testimony or an opinion that Prism and/or AT&T manipulated the AT&T Settlement Agreements to attribute the entire settlement amount to a license for the asserted patents in order to influence Sprint's and the other carriers' litigations.

Denied.

17) Sprint may not present argument, testimony, evidence or expert opinion regarding a smallest salable patent practicing unit.

Denied as moot. The Court has ruled on this issue in a concurrent order related to Filing Nos. 329, 230, and 333.

18) Sprint may not present argument, testimony, evidence or expert opinion regarding the cost of SIM cards or non-volatile memory as the basis for a damages calculation.

Denied as moot. The Court has ruled on this issue in a concurrent order related to Filing Nos. 329, 230, and 333.

19) Sprint may not introduce as evidence or present any argument, testimony or expert opinion regarding the document bearing Bates-number SPRINTPR00091538-539.

Denied as moot. The Court has ruled on this issue in a concurrent order related to Filing Nos. 329, 230, and 333.

21) Consistent with F.R.E. 408, the parties will not offer testimony, evidence or argument regarding settlement communications between Prism and any of the wireless carriers (i.e., AT&T, Sprint, T-Mobile, USCC and Verizon).

Granted as to Sprint, T-Mobile, USCC, and Verizon. Deferred until trial as to AT&T.

## II. SPRINT'S MOTIONS *IN LIMINE*

1) Prism will not provide testimony, other evidence, or argument regarding the Prism v. AT&T Settlement and License Agreement or testimony, other evidence, or argument revealing the identity of AT&T as the licensee to the agreement.

Denied.

2) Prism will not offer lay opinion testimony from Mr. Duman that Prism would have offered Sprint a license to the Asserted Patents equal to five percent of Sprint's cost savings achieved by leasing as opposed to buying its backhaul networks; and Prism will not offer expert opinion testimony from Mr. Duman that Prism would have offered Sprint a license to the Asserted Patents equal to five percent of Sprint's cost savings achieved by leasing as opposed to buying its backhaul networks.

Denied.

3) Prism will not offer testimony, other evidence, or argument regarding any documents filed with the Securities and Exchange Commission authored by anyone other than Sprint and its affiliates or Prism and its affiliates.

Granted.

4) With the exception of documents specifically referenced in the body of the parties' expert reports, the parties will not offer testimony, other evidence, or argument

regarding any contract between any backhaul provider and any party.<sup>2</sup>

Denied.

5) Prism will not offer testimony, other evidence, or argument regarding any statement to the Federal Communications Commission authored by anyone other than Sprint.

Granted.

6) Prism will not offer testimony, other evidence, or argument regarding Sprint's data revenue, voice revenue, overall revenues, overall profits, or market value.

Deferred until trial. The Court will allow Prism to use revenue-based information only in the event that Sprint relies upon specific revenue-based theories.

7) Prism will not offer testimony, other evidence, or argument speculating that potentially-relevant Sprint documents exist but were not produced by Sprint in this case.

Granted as to both parties.

8) Prism will not offer testimony, other evidence, or argument regarding the opinions or statements made or reports served in the Carrier Defendant Cases by any expert.

Granted as to both parties.

9) Prism will not offer testimony, other evidence, or argument regarding the technical operation of the accused networks in Prism's Carrier Defendant Cases not of record in this case.

Deferred until trial.

---

<sup>2</sup> The Court has reworded the language of this motion. The original text read as follows: Prism will not offer testimony, other evidence, or argument regarding any contract between any backhaul provider and any party other than Sprint and Prism's experts may only rely on documents specifically referenced in the body of their expert reports. Filing No. 363, at 3.

10) Prism will not offer testimony, other evidence, or argument regarding any settlement discussions, or lack thereof, between Prism and Sprint or the other remaining defendants in the Carrier Defendant Cases.

Deferred until trial.

11) Prism will not offer testimony, other evidence, or argument regarding reexaminations of the '288 patent by the United States Patent and Trademark Office.

Denied.

DATED this 8th day of June, 2015.

BY THE COURT:

/s/ Lyle E. Strom

---

LYLE E. STROM, Senior Judge  
United States District Court

# The United States of America



## The Director of the United States Patent and Trademark Office

*Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.*

*Therefore, this*

## United States Patent

*Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America for the term set forth below, subject to the payment of maintenance fees as provided by law.*

*If this application was filed prior to June 8, 1995, the term of this patent is the longer of seventeen years from the date of grant of this patent or twenty years from the earliest effective U.S. filing date of the application, subject to any statutory extension.*

*If this application was filed on or after June 8, 1995, the term of this patent is twenty years from the U.S. filing date, subject to any statutory extension. If the application contains a specific reference to an earlier filed application or applications under 35 U.S.C. 120, 121 or 365(c), the term of the patent is twenty years from the date on which the earliest application was filed, subject to any statutory extensions.*

A handwritten signature in black ink, appearing to read "James M. Rogan".

*Director of the United States Patent and Trademark Office*

Trial Exhibit

**TX 1**

Case No. 8:12-CV-123-LES-TDT

TX0001-0001

## **NOTICE**

*If the application for this patent was filed on or after December 12, 1980, maintenance fees are due three years and six months, seven years and six months, and eleven years and six months after the date of this grant, or within a grace period of six months thereafter upon payment of a surcharge as provided by law. The amount, number of timing of the maintenance fees required may be changed by law or regulation. Unless payment of the applicable maintenance fee is received in the United States Patent and Trademark Office on or before the date the fee is due or within a grace period of six months thereafter, the patent will expire as of the end of such grace period.*



US008127345B2

(12) **United States Patent**  
Gregg et al.

(10) **Patent No.:** US 8,127,345 B2  
(45) **Date of Patent:** \*Feb. 28, 2012

(54) **METHOD AND SYSTEM FOR MANAGING ACCESS TO PROTECTED COMPUTER RESOURCES PROVIDED VIA AN INTERNET PROTOCOL NETWORK**

(75) Inventors: **Richard L. Gregg**, Elkhorn, NE (US);  
**Sandeep Giri**, Omaha, NE (US);  
**Timothy C. Goeke**, Elkhorn, NE (US)

(73) Assignee: **Prism Technologies LLC**, Omaha, NE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 585 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **11/978,919**

(22) Filed: **Oct. 30, 2007**

(65) **Prior Publication Data**

US 2008/0066168 A1 Mar. 13, 2008

**Related U.S. Application Data**

(63) Continuation of application No. 10/230,638, filed on Aug. 29, 2002, now Pat. No. 7,290,288, which is a continuation-in-part of application No. 08/872,710, filed on Jun. 11, 1997, now Pat. No. 6,516,416.

(51) **Int. Cl.**

**G06F 7/04** (2006.01)

**G06F 15/16** (2006.01)

**G06F 17/30** (2006.01)

**H04L 29/06** (2006.01)

(52) **U.S. Cl.** ..... 726/7; 726/4; 726/5

(58) **Field of Classification Search** ..... 726/7, 4, 726/5

See application file for complete search history.

(56) **References Cited**

U.S. PATENT DOCUMENTS

4,691,355 A 9/1987 Wirstrom et al.  
(Continued)

FOREIGN PATENT DOCUMENTS

EP 94111581.8 2/1995  
(Continued)

OTHER PUBLICATIONS

*Prism Technologies LLC, v. Verisign, Inc., et al.; Civil Action No. 05-214 JJF; Defendants' Second Supplemental Joint 35 U.S.C. § 282 Notice; Mar. 12, 2007; 7 pages; Exhibit A, pp. 1-80.*

(Continued)

*Primary Examiner — Kambiz Zand*

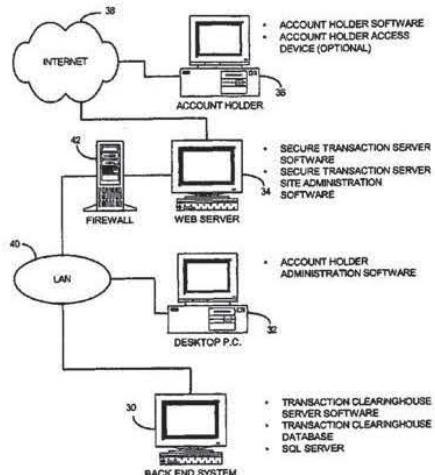
*Assistant Examiner — Aubrey Wyszynski*

(74) *Attorney, Agent, or Firm — Martin & Ferraro, LLP*

(57) **ABSTRACT**

A method and system for controlling access, by an authentication server, to protected computer resources provided via an Internet Protocol network that includes storing (i) a digital identification associated with at least one client computer device, and (ii) data associated with the protected computer resources in at least one database associated with the authentication server; authenticating, by the authentication server, the digital identification forwarded by at least one access server; authorizing, by the authentication server, the at least one client computer device to receive at least a portion of the protected computer resources requested by the at least one client computer device, based on the stored data associated with the requested protected computer resources; and permitting access, by the authentication server, to the at least the portion of the protected computer resources upon successfully authenticating the digital identification and upon successfully authorizing the at least one client computer device.

92 Claims, 27 Drawing Sheets



TX0001-0003

# US 8,127,345 B2

Page 2

## U.S. PATENT DOCUMENTS

4,694,492 A	9/1987	Wirstrom et al.	5,740,361 A	4/1998	Brown
4,796,220 A	1/1989	Wolfe	5,754,864 A	5/1998	Hill
4,864,494 A	9/1989	Kobus, Jr.	5,757,907 A	5/1998	Cooper et al.
4,885,789 A	12/1989	Burger et al.	5,761,306 A	6/1998	Lewis
4,907,268 A	3/1990	Bosen et al.	5,761,309 A	6/1998	Ohashi et al.
4,916,738 A	4/1990	Chandra et al.	5,761,649 A	6/1998	Hill
4,932,054 A	6/1990	Chou et al.	5,765,152 A	6/1998	Erickson
4,935,962 A	6/1990	Austin	5,774,552 A	6/1998	Grimmer
4,962,449 A	10/1990	Schlesinger	5,778,071 A	7/1998	Caputo et al.
4,977,594 A	12/1990	Shear	5,781,723 A	7/1998	Yee et al.
5,032,979 A	7/1991	Hecht et al.	5,784,464 A	7/1998	Akiyama et al.
5,060,263 A	10/1991	Bosen et al.	5,790,677 A	8/1998	Fox et al.
5,081,676 A	1/1992	Chou et al.	5,793,868 A	8/1998	Micali
5,103,476 A	4/1992	Waite et al.	5,809,144 A	9/1998	Sirbu et al.
5,199,066 A	3/1993	Logan	5,815,665 A	9/1998	Teper et al.
5,204,961 A	4/1993	Barlow	5,841,970 A *	11/1998	Tabuki ..... 726/2
5,222,133 A	6/1993	Chou et al.	5,878,142 A	3/1999	Caputo et al.
5,222,134 A	6/1993	Waite et al.	5,889,958 A	3/1999	Willens
5,229,764 A *	7/1993	Matchett et al.	5,910,987 A	6/1999	Ginter et al.
5,235,642 A	8/1993	Wobber et al.	5,922,074 A	7/1999	Richard et al.
5,237,614 A	8/1993	Weiss	5,926,624 A	7/1999	Katz et al.
5,247,575 A	9/1993	Sprague et al.	5,930,804 A	7/1999	Yu et al.
5,291,598 A	3/1994	Grundy	5,943,423 A	8/1999	Muflic
5,315,657 A	5/1994	Abadl et al.	5,969,316 A	10/1999	Greer et al.
5,347,580 A	9/1994	Molva et al.	5,982,898 A	11/1999	Hsu et al.
5,349,643 A	9/1994	Cox et al.	5,987,232 A	11/1999	Tabuki
5,357,573 A	10/1994	Walters	5,999,711 A	12/1999	Misra et al.
5,371,794 A	12/1994	Diffee et al.	6,003,135 A	12/1999	Bialick et al.
5,373,561 A	12/1994	Haber et al.	6,005,939 A	12/1999	Fortenberry et al.
5,375,240 A	12/1994	Grundy	6,006,332 A	12/1999	Rabne et al.
5,379,343 A	1/1995	Grube et al.	6,021,202 A	2/2000	Anderson et al.
5,414,844 A *	5/1995	Wang	6,035,402 A	3/2000	Vaeth et al.
5,416,842 A	5/1995	Aziz	6,041,411 A	3/2000	Wyatt
5,428,745 A	6/1995	De Brujin et al.	6,044,471 A	3/2000	Colvin
5,442,708 A	8/1995	Adams, Jr. et al.	6,047,376 A	4/2000	Hosoe
5,444,782 A	8/1995	Adams et al.	6,075,860 A	6/2000	Ketcham
5,455,953 A	10/1995	Russell	6,088,451 A	7/2000	He et al.
5,483,596 A	1/1996	Rosenow et al.	6,212,634 B1	4/2001	Geer, Jr. et al.
5,485,409 A	1/1996	Gupta et al.	6,219,790 B1	4/2001	Lloyd et al.
5,490,216 A	2/1996	Richardson, III	6,223,984 B1	5/2001	Renner et al.
5,491,804 A	2/1996	Heath et al.	6,226,744 B1	5/2001	Murphy et al.
5,497,421 A	3/1996	Kaufman et al.	6,249,873 B1	6/2001	Richard et al.
5,499,297 A	3/1996	Boebert	6,377,994 B1 *	4/2002	Ault et al. ..... 709/229
5,502,766 A	3/1996	Boebert et al.	6,510,236 B1	1/2003	Crane et al.
5,502,831 A	3/1996	Grube et al.	6,516,416 B2	2/2003	Gregg et al.
5,511,122 A	4/1996	Atkinson	6,553,492 B1	4/2003	Hosoe
5,535,276 A	7/1996	Ganesan	7,117,376 B2	10/2006	Grawrock
5,539,828 A	7/1996	Davis	7,290,288 B2	10/2007	Gregg et al.
5,546,463 A	8/1996	Caputo et al.	2011/0061097 A1	3/2011	Gregg et al.
5,572,673 A	11/1996	Shurts			
5,588,059 A	12/1996	Chandos et al.			
5,590,197 A	12/1996	Chen et al.			
5,590,199 A	12/1996	Krajewski, Jr. et al.			
5,592,553 A	1/1997	Guski et al.			
5,604,804 A	2/1997	Micali			
5,606,615 A	2/1997	Laponte et al.			
5,623,637 A	4/1997	Jones et al.			
5,629,980 A	5/1997	Stefik et al.			
5,634,012 A	5/1997	Stefik et al.			
5,657,390 A	8/1997	Elgamal et al.			
5,659,616 A	8/1997	Sudia			
5,666,411 A	9/1997	McCarty			
5,666,416 A	9/1997	Micali			
5,677,953 A	10/1997	Dolphin			
5,677,955 A	10/1997	Doggett et al.			
5,679,945 A	10/1997	Renner et al.			
5,687,235 A	11/1997	Perlman et al.			
5,696,824 A	12/1997	Walsh			
5,699,431 A	12/1997	Van Ocschot et al.			
5,706,427 A	1/1998	Tabuki			
5,708,780 A	1/1998	Levergood et al.			
5,710,884 A *	1/1998	Dedrick	909/217		
5,715,314 A	2/1998	Payne et al.			
5,717,756 A *	2/1998	Coleman	713/155		
5,717,757 A	2/1998	Micali			
5,717,758 A	2/1998	Micali			
5,721,781 A	2/1998	Deo et al.			
5,724,424 A	3/1998	Gifford			

## FOREIGN PATENT DOCUMENTS

EP	96306390.4	9/1996
JP	07231159	9/1995
JP	07231160	9/1995
JP	10285156	10/1998
WO	WO94/26044	11/1994
WO	WO96/07256	3/1996
WO	PCT/US00/03489	2/2000

## OTHER PUBLICATIONS

- Prism Technologies LLC, v. Verisign, Inc., et al.; Civil Action No. 05-214-JJF; Plaintiff's First Amended Complaint for Patent Infringement and Demand for Jury Trial; Jun. 22, 2005; 7 pages.*
- Prism Technologies LLC, v. Verisign, Inc., et al.; Civil Action No. CA 05-00214 JJF; Plaintiff's Second Amended Complaint for Patent Infringement and Demand for Jury Trial; Aug. 11, 2006; 7 pages.*
- Prism Technologies LLC., v. Research in Motion, Ltd., et al.; Case No. 8:08-CV-537; Complaint; Dec. 29, 2008; pp. 1-5.*
- Prism Technologies LLC., v. Research in Motion, Ltd.; Case No. 8:08-cv-00537-LES-TDT; Joint Claim Construction Statement; Document No. 72; Oct. 16, 2009; pp. 1-6.*
- Prism Technologies LLC., v. Research in Motion, Ltd., et al.; Case No. 8:08-cv-00537-LES-TDT; Plaintiff's Disclosure of Asserted Claims and Preliminary Infringement Contentions Regarding Defendant Microsoft Corporation; Jun. 26, 2009; 4 pages.*
- Prism Technologies LLC., v. Research in Motion, Ltd., et al.; Case No. 8:08-cv-00537-LES-TDT; Plaintiff's Disclosure of Asserted*

Claims and Preliminary Infringement Contentions Regarding Defendant Research in Motion, Ltd.; Jun. 26, 2009; 4 pages.

*Prism Technologies LLC., v. Research in Motion, Ltd., et al.; Case No. 8:08-cv-00537-LES-TDT; Defendant Research in Motion, Ltd.'s Amended Invalidity Contentions; Sep. 18, 2009; 7 pages; Akiyama Chart, 65 pages; Yu Chart, 72 pages; Tabuki Chart, 52 pages; Teper Chart, 54 pages; Grawrock Chart, 39 pages; Crane Chart, 37 pages; Murphy Chart, 38 pages; He Chart, 45 pages; Ketcham Chart, 74 pages; Krajewski Chart, 127 pages; DCE Chart (redacted), 192 pages; SiteMinder Chart, 61 pages; Handbook of Applied Cryptography Chart, 124 pages; Kerberos V5 Chart, 46 pages.*

*Prism Technologies LLC., v. Research in Motion, Ltd.; No. 8:08-CV-537; Research in Motion, Ltd.'s Response to Plaintiff Prism Technologies LLC's Opening Claim Construction Brief; Document 94; Dec. 4, 2009; 50 pages.*

*Prism Technologies LLC., v. Research in Motion, Ltd.; No. 8:08-CV-537; Index of Evidence in Support of Research in Motion, LTD.'s Response to Plaintiff Prism Technologies LLC's Opening Claim Construction Brief; Document 95; Dec. 4, 2009; 4 pages; Exhibit A, 4 pages; Exhibit C, 4 pages; Exhibit D, 3 pages; Exhibit E, 68 pages; Exhibit F, 24 pages; Exhibit G, 27 pages; Exhibit L, 42 pages; Exhibit M, 7 pages; Exhibit N, 3 pages.*

*Prism Technologies LLC., v. Research in Motion, Ltd.; Case No. 8:08-cv-00537-LES-TDT; Plaintiff's Amended Disclosure of Asserted Claims and Preliminary Infringement Contentions; Feb. 5, 2010; 6 pages; Exhibit A, cover page and pp. 1-134.*

*Prism Technologies LLC., v. Research in Motion, Ltd.; Case No. 8:08-cv-00537-LES-TDT; Second Supplemental Responses to Research in Motion, Ltd.'s Interrogatories Nos. 5, 6 and 8; Feb. 16, 2010; 12 pages.*

*Prism Technologies, LLC, v. Research in Motion, Ltd; 8:08CV537; Order; Document No. 132; Feb. 22, 2010; 1 page.*

*Prism Technologies, LLC, v. Research in Motion, Ltd; 8:08-CV-537; Plaintiff Prism Technologies' Reply Brief on Claim Construction; Document No. 154; Mar. 22, 2010; 34 pages.*

*Prism Technologies, LLC, v. Research in Motion, Ltd; 8:08-CV-537; Index of Evidence in Support of Plaintiff Prism Technologies' Reply Brief on Claim Construction; Document No. 155; Mar. 22, 2010; 3 pages; Exhibit D, 17 pages; Exhibit E, 3 pages; Exhibit F, 11 pages; Exhibit G, 69 pages; Exhibit H, 2 pages.*

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Verified Complaint Under Section 337 of the Tariff Act of 1930, As Amended; 26 pages; Exhibit 2, 11 pages; Exhibit 3, 31 pages; Exhibit 4, 31 pages; Exhibit 5, 1 page; Exhibit 6, 4 pages; Exhibit 7, 31 pages; Exhibit 8, 2 pages; Exhibit 9, 92 pages; Exhibit 10, 4 pages; Exhibit 11, 92 pages; Exhibit 12, 56 pages; Exhibit 13, 17 pages; Exhibit 26, 2 pages; Exhibit 29, 10 pages; Exhibit 30, 1 page; Exhibit 31, 1 page; Exhibit 32, 4 pages; Exhibit 34, 19 pages; Exhibit 35, 3 pages; Exhibit 36, 1 page; Exhibit 37, 169 pages; Letter Submitting Verified Complaint to the International Trade Commission; 2 pages; Letter Requesting Confidential Treatment of Exhibits; 2 pages; Dec. 2, 2009.

In re Certain Authentication Systems, Including Software and Handheld Electronic Devices; Public Version of Confidential Submissions; 3 pages; Exhibit 19, 3 pages; Exhibit 20, 4 pages; Exhibit 39, 2 pages; Dec. 18, 2009.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Response of Respondents Research in Motion Limited and Research in Motion Corporation to the Verified Complaint and Notice of Investigation; 27 pages; Exhibit A, 21 pages; Exhibit A-1, 421 pages; Exhibit A-2, 145 pages; Exhibit B, 37 pages; Exhibit C, 47 pages; Exhibit D, 35 pages; Exhibit E, 49 pages; Exhibit F, 37 pages; Exhibit G, 34 pages; Exhibit H, 28 pages; Jan. 20, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Complainant Prism Technologies' Supplemental Response to Research in Motion Corporation's Interrogatory No. 4; 6 pages; Feb. 26, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697;

Complainant Prism Technologies' Amended Response to Research in Motion Corporation's Interrogatory No. 4; 8 pages; Mar. 11, 2010. In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Complainant Prism Technologies' Amended Responses to Research in Motion Limited's Interrogatories Nos. 13 and 16; 9 pages; Mar. 11, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Complainant Prism Technologies' Supplemental Response to Respondent Research in Motion Limited's Interrogatories Nos. 13-19; 87 pages; Mar. 24, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Respondent Research in Motion Corporation's Supplemental Response to Prism's Interrogatory No. 25; 9 pages; Mar. 26, 2010. In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Respondent Research in Motion Limited's Supplemental Response to Prism's Interrogatory No. 25; 9 pages; Mar. 26, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; 4 pages; Mar. 29, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Memorandum in Support of Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; Redacted Version; 10 pages; Mar. 29, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Statement of Material Facts for Which There is No Genuine Issue Accompanying Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; Redacted Version; 7 pages; Mar. 29, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Declaration of Christopher R. Lire in Support of Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; 3 pages; Exhibit C, 98 pages; Exhibit E, 10 pages; Exhibit F, 6 pages; Mar. 29, 2010.

Aboba, B., et al.; "RADIUS Authentication Client MIB;" Request for Comments: 2618; Jun. 1999; 14 pages.

Berners-Lee, T., et al.; "Hypertext Transfer Protocol—HTTP/1.0;" Request for Comments: 1945; May 1996; 60 pages.

Braden, R.; "Requirements for Internet Hosts—Communication Layers;" Request for Comments: 1122; Oct. 1989; 116 pages.

Bruno, Lee; "Software & Security Netegrity's Siteminder Software Lets Net Managers Get Centered on Security;" Data Communications, vol. 26, No. 1; 2 pages.

Bryant, Bill; "Designing an Authentication System: a Dialogue in Four Scenes;" Massachusetts Institute of Technology; Feb. 1997; 18 pages.

Burati, M., et al.; "User-to-User Authentication—Functional Specification;" Request for Comments: 91.0; Jan. 1996; 9 pages.

Business Wire; Secure Computing Announces Immediate Availability of Sidewinder 3.0; Security Server Employs Fully Integrated Perimeter Security, Ipsec Interoperable Encryption, Strong User Authentication, and E-mail Content Filtering. Sep. 17, 1996; 2 pages. Dascom; "Integration of DCE/Kerberos with Public Key Infrastructure using the Cryptographic Message Syntax (PKINIT/CMS); Mar. 30, 1998; 27 pages.

Doan, Amy; "Remote Access Vendors Try RADIUS;" InfoWorld; Sep. 23, 1996; 1 page.

Erdos, Marlena E., et al.; "Extending the OSF DCE Authorization System to Support Practical Delegation;" to appear in PSRG Workshop on Network and Distributed System Security; Feb. 11-12, 1993; 8 pages.

- Estrin, Deborah, et al.; "Visa Scheme for Inter-Organization Network Security;" IEEE Symposium on Security and Privacy; Apr. 1987; pp. 174-183.
- Gligor, Virgil D., et al.; "On Inter-realm Authentication in Large Distributed Systems;" Proceedings of the 1992 IEEE Symposium on Security and Privacy; 1992; pp. 2-17.
- Hornstein, Ken; "Kerberos FAQ, v2.0;" <http://wwwfaqs.org/faqs/kerberos-faq/general/>; Sep. 17, 2009; 51 pages.
- Interlink AAA Server Software: Authentication Guide; "LDAP and ProLDAP;" 2000; 16 pages.
- Interlink Networks AAA Server; "Administrator's Guide;" 2000; 88 pages.
- Interlink Networks AAA Server; "Getting Started;" 2000; 31 pages.
- Kohl, John T., et al.; "The Evolution of the Kerberos Authentication Service;" appeared in Distributed Open Systems; 1994; 15 pages.
- Krishnamurthy, Sriekha, et al.; "Digital Security Forensics SiteMinder—A Portal Security Management Tool;" White Paper; Ver. No. 1.0; Mar. 18, 2002; 25 pages.
- Lucent Technologies; "RADIUS Remote Authentication Dial-in User Service;" Jun. 1999; 6 pages.
- Menezes, A., et al.; "Handbook of Applied Cryptography;" CRC Press, Inc.; 1997; cover page and pp. 1-319, 321-383, 385-541, 543-661, and 663-780.
- Merit AAA Server; "Differentiating Authentication Policy by Hunt Group;" 5 pages.
- Merit AAA Server; "Distributed Authentication/Authorization;" 3 pages.
- Merit AAA Server; "Installation Instructions for MichNet Dial-in;" 7 pages.
- Merit AAA Server; "LAS—Local Authorization Serve;" 6 pages.
- Mullan, S.; "DCE Interoperability With Kerberos—Functional Specification;" Request for Comments: 92.0; Jan. 1996; 27 pages.
- Nelson, Dave, et al.; "Current Meeting Report—Minutes of the Remote Authentication Dial-In User Services Working Group (radius);" Mar. 1996; 6 pages.
- Netegrity; "SiteMinder Frequently Asked Questions;" [http://web.archive.org/web/19990508041248/www.netegrity.com/product/siteminder\\_faq\\_s.html](http://web.archive.org/web/19990508041248/www.netegrity.com/product/siteminder_faq_s.html); May 8, 1999; 8 pages.
- Pato, Joseph N.; "Distributed Computing Environment (OSF DCE) Security Architecture;" 14 Forum; Jan. 18-27, 1993; 32 pages.
- Pato, J.; "Extending the DCE Authorization Model to Support Practical Delegation (Extended Summary);" Request for Comments: 3.0; Jun. 1992; 18 pages.
- Pato, J.; "A Generic Interface for Extended Registry Attributes;" Request for Comments: 6.0; Jun. 1992; 23 pages.
- Pato, J.; "Hierarchical Trust Relationships for Inter-Cell Authentication;" Request for Comments: 7.0; Jul. 1992; 7 pages.
- Rigney, C., et al.; "RADIUS Accounting draft-ietf-radius-accounting-00.txt;" Jul. 1995; 22 pages.
- Stevens, W. Richard; "TCP/IP Illustrated: the protocols;" vol. 1; May 1994; cover page and pp. 33-39.
- Weiner, Bruce; "Netegrity SiteMinder 4.61 with Microsoft Active Directory AuthMark Performance;" Apr. 18, 2002; 4 pages.
- Woo, Thomas Y.C., et al.; "Authentication for Distributed Systems;" to appear in Internet Besieged: Countering Cyberspace Scofflaws; 1997; 30 pages.
- Zorn, G. et al.; "RADIUS Authentication Server MIB;" Request for Comments: 2619; Jun. 1999; 16 pages.
- Anderson et al.; RFC 68.2-DCE 1.2.2 Public Key Login—Functional Specification; Feb. 1996; 44 pages.
- Braden, R., et al.; RFC 1636—Report of IAB Workshop on Security in the Internet Architecture; Jun. 1994; 49 pages.
- Bridges, S.; Strong Authentication Questions; Mar. 1996; 3 pages.
- Coe, et al. D.; Developing and Deploying Corporate Cryptographic Systems; Jul. 1995; 13 pages.
- Community Connexion; Mailing list archives; Community Connexion Announces Stronghold Version 1.2; Community Connexion, Inc.; Jul. 16, 1996.
- Comp.Security.UNIX; password encryption (security) over networks; Google Groups; Jun. 1994.
- Finseth, C.; RFC 1492—An Access Control Protocol, Sometimes Called TACACS; Jul. 1993; 21 pages.
- Franks, et al.; RFC 2069—An Extension to HTTP: Digest Access Authentication; Jan. 1997; 17 pages.
- Fruth, P.; Product Update: CE Software Quickmail 3.5; Nov. 1995; 3 pages.
- Gaskell, et al.; RFC 71.0—Improved Security for Smart Card Use in DCE; Open Software Foundation Request for Comments 71.0; Feb. 1995; 9 pages.
- Gaskell, Gary Ian; "Integrating Smart Cards into Kerberos;" Feb. 2000; 128 pages.
- Haller, N., et al.; RFC 1704—On Internet Authentication; Oct. 1994; 16 pages.
- Howes, et al.; RFC 1823—The LDAP Application Program Interface; Aug. 1995; 21 pages.
- Howes, T.; CITI Technical Report 95-8; The Lightweight Directors Access Protocol: X.500 Lite; Jul. 1995; 11 pages.
- Hunwick, T.; RFC 8.2—Security Requirements for DCE; Aug. 1996; 64 pages.
- Itoi, et al.; CITI Technical Report 98-7; Smartcard Integration and Kerberos V5; Dec. 1998; 11 pages.
- Kaufman, C.; RFC 1507—DASS, Distributed Authentication Security Service; Sep. 1993; 119 pages.
- Kemp, D.; The Public Key Login Protocol; <draft-kemp-auth-pklogin-01.txt>; Aug. 13, 1996; 18 pages.
- Kemp, D.; The Public Key Login Protocol; <draft-kemp-auth-pklogin-02.txt>; Nov. 26, 1996; 18 pages.
- Kohl, et al.; RFC 1510—The Kerberos Network Authentication Service (V5); Sep. 1993; 105 pages.
- Kotanchik, J.; RFC 59.0—Kerberos and Two-Factor Authentication; Mar. 1994; 11 pages.
- Lai, et al.; Endorsements, Licensing, and Insurance for Distributed System Services; Information Services Institute University of Southern California; Nov. 1994; pp. 170-175.
- Linn, J.; RFC 1508—Generic Security Service Application Program Interface; Sep. 1993; 46 pages.
- Myers, J.; RFC 1731—IMAP4 Authentication Mechanisms; Dec. 1994; 6 pages.
- Netegrity; Netegrity Unveils Industry's First Enterprise-Wide, Integrated Network Security Management System; Netegrity, Inc.; Oct. 15, 1996; 2 pages.
- Netegrity; SiteMinder Product/Technology Backgrounder; Netegrity, Inc.; 1996; 3 pages.
- Netegrity; SiteMinder Authentication Server for Windows NT; Netegrity, Inc.; 1996.
- Netscape; Netscape Communicator Supports Smart Cards and Tokens So Mobile Users Can Safely Access Corporate Networks Remotely; Aug. 1997; 3 pages.
- Newman, et al.; Kerberos: An Authentication Service for Computer Networks; reprinted from IEEE Communications Magazine, vol. 32, No. 9, pp. 33-38; Sep. 1994; 11 pages.
- Parker, et al.; Sesame Technology Version 4 Overview; Issue 1; Dec. 1995; 90 pages.
- Pato, J.; RFC 26.0—Using Pre-Authentication to Avoid Password Guessing Attacks; Open Software Foundation Request for Comments 26.0; Jun. 1993; 7 pages.
- Regents of the University of Michigan; The SLAPD and SLURPD Administrators Guide, University of Michigan, Release 3.3; Apr. 1996; 100 pages.
- Rigney, C.; RADIUS Accounting draft-ietf-radius-accounting-01.txt; Nov. 1995; 54 pages.
- Rigney, C.; RADIUS Accounting; draft-ietf-radius-accounting-02.txt; Feb. 1996; 46 pages.
- Rigney, C.; RADIUS Accounting; draft-ietf-radius-accounting-03.txt; May 1996; 50 pages.
- Rigney, C.; RADIUS Accounting; draft-ietf-radius-accounting-04.txt; Jun. 1996; 54 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-00.txt; May 1995; 70 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-01.txt; Nov. 1995; 79 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-02.txt; Feb. 1996; 133.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-radius-03.txt; May 1996; 69 pages.

- Rigney, et al.; RFC 2058—Remote Authentication Dial in User Service (RADIUS); Jan. 1997; 64 pages.
- Rigney, et al.; RFC 2138—Remote Authentication Dial in User Service (RADIUS); Apr. 1997; 66 pages.
- Rigney, C.; RFC 2139—RADIUS Accounting; Apr. 1997; 25 pages.
- RISS; Getting Connected; Regional Information Sharing Systems; Jun. 27, 2000; 16 pages.
- RISS; Network Fundamentals; Regional Information Sharing Systems; Jun. 26, 2000; 17 pages.
- Rubin, A.D.; Independent One-Time Passwords, Proceedings of the Fifth USENIX UNIX Security Symposium; Jun. 1995; 11 pages.
- Salz, R.; RFC 100.0—DCE and Fortezza; Jan. 1997; 6 pages.
- Salz, R.; RFC 63.3—DCE 1.2 Contents Overview; Oct. 1996; 15 pages.
- Schroeder, W.; Kerberos/DCE, the Secure Shell, and Practical Internet Security; Oct. 1996; 10 pages.
- The Open Group; DCE, Distributing Computing Environment Overview; 1996; 7 pages.
- The Open Group; DCE, Distributing Computing Environment, OSF DCE 1.2.2 New Features; 1996; 5 pages.
- The Open Group; Draft Technical Standard, DCE 1.2.3 Public Key Certificate Login (Draft 0.8 for Company Review); Aug. 1998; 52 pages.
- The Open Group; Press Release: The Open Group and The Securities Industry Middleware Council Announce Security Solution for Wall Street—*Integrating Smart Cards and DCE*; Jun. 1998; 3 pages.
- Tung; The Moron's Guide to Kerberos, Version 1.2.2; Dec. 1996; 11 pages.
- U.S. Department of Commerce/National Institute of Standards and Technology; FIPS PUB 190—Guideline for the Use of Advanced Authentication Technology Alternatives; Sep. 1994; 47 pages.
- Wallace, B.; RADIUS to secure remote access; Apr. 1995; 3 pages.
- Warner, M.; RFC 85.0—Improved Public Key Login Protocols for DCE; Oct. 1995; 17 pages.
- Westlaw; Hudgins-Bonafield, Christy; Bridging The Business-to-Business Authentication Gap; Network Computing; Jul. 1997.
- Workshop on Network and Distributed Systems Security; Krajewski, Jr., Marjan; Smart Card Augmentation of Kerberos; Feb. 1993; pp. 119-123.
- Yeong, et al.; RFC 1777—Lightweight Directory Access Protocol; Mar. 1995; 21 pages.
- Request for Ex Parte Reexamination of U.S. Patent No. 7,290,288, dated Jun. 4, 2009, pp. 1-148. Exhibit I, cover page and pp. 1-54. Exhibit J, cover page and pp. 1-90. Exhibit K, cover page and pp. 1-74. Exhibit L, cover page and pp. 1-32. Exhibit M, cover page and pp. 1-27. Exhibit N, cover page and pp. 1-27.
- Microsoft Corporation's Preliminary Invalidity Contentions; *Prism Technologies, LLC v. Research in Motion, LTD.*, and Microsoft Corporation; Case No. 8:08-cv-537; dated Jul. 24, 2009; 8 pages; Exhibit A, Table of references, 1 page; Exhibit B, Claim charts, 68 pages. Defendant Research in Motion, LTD.'s Preliminary Invalidity Contentions; *Prism Technologies, LLC v. Research in Motion, Ltd.*, and Microsoft Corporation; Case No. 8:08-cv-00537-LES-TDT; dated Jul. 24, 2009; 5 pages; Exhibit A, RIM Preliminary Invalidity Contentions Chart, 210 pages; Exhibit B, Willens, S., et al., RADIUS, draft-ietf-nasreq-radius-01.txt, RFC2058, Apr. 10, 2002, 33 pages. Abadl et al.; Authentication and Delegation with Smart-Cards; Jul. 1992.
- Ahuja, V.; Network and Internet Security; 1996.
- Anderson et al.; RFC 68.2—DCE 1.2.2 Public Key Login—Functional Specification; Feb. 1996.
- Anderson et al.; RFE 68.1—DCE 1.2 Public-Key Login—Functional Specification; Feb. 1995.
- Andresen, M.; Interoperable Security; Dec. 1996.
- Arsenley, M.; How are X.509 Certificates Used in User Authentication and Authorization; Feb. 2002.
- Atkinson, R.; RFC 1826—IP Authentication Header; Aug. 1995.
- Atkinson, R.; RFC 1827—IP Encapsulating Security Payload (ESP); Aug. 1995.
- Baker et al.; RFC 2082—RIP-2 MD5 Authentication; Jan. 1997.
- Battelle; Battelle Press Releases; Battelle, Cybermark Complete Successful Testing of Digital Cash Transfer from Smart Card; Feb. 7, 2007; Battelle Memorial Institute; (VERI-1607108-VERI-1607110).
- Battelle; Solutions Update; Technology Development, Product Development, and Technology Commercialization; The chemical Industry pools environmental technology dollars; Fall 1996; (VERI-1607111-VERI-1607122).
- Braden et al.; RFC 1636—Report of IAB Workshop on Security in the Internet Architecture Feb. 8-10, 1994. (Jun. 1994).
- Bridges, S.; Strong Authentication Questions; Mar. 1996.
- BTAS and the World Wide Web: An Introduction and Technical Overview; DRAFT; Apr. 1997.
- Business Wire; Secure Computing Corp. Announces Agreement with Security Dynamics Technologies, Inc. to Provide Enhanced Security for Computer Networks; Jan. 23, 1996.
- Byte; Kay, Russell; Jun. 1994/Special Report/Distributed and Secure; When you distribute information and processing, you also delegate security responsibility. Good access controls, eyes-open administration, and communications encryption can make all the difference; BYTE.com; CMP Media LLC; (VERI-1605576-VERI-1605587).
- Carr, J.; The Price of Access Is Eternal Vigilance—Security Sells Itself as Remote Connections Spread the Risk of Unauthorized Access to Corporate Data; Oct. 1995.
- CCITT/ISO X.500 The Directory—Overview of Concepts, Models & Services; Dec. 2001.
- Choudhury, A. et al.; Copyright Protection for Electronic Publishing Over Computer Networks; IEEE Network; May/Jun. 1995.
- Chrysalis; Chrysalis-ITS; Canadian Department of National Defense Installs Integrated information Security solutions from Chrysalis; Mergent International, and Northern Telecom (Nortel) Top Information Security Vendors Combine Solutions to Provide a High Level of Security to DND in Ottawa; Rocky Hill, Conn. (Apr. 19, 1996); (VERI-1605384-VERI-1605385).
- Chrysalis; Chrysalis-ITS; Safeguard the Keys to Electronic Commerce; Chrysalis-ITS, Inc.; (VERI-1605091-VERI-1605092).
- Chrysalis; Seminerio, Maria; Chrysalis-ITS; Chrysalis to debut encryption token card; PC Week OnLine Oct. 30, 1996 (reprinted); (VERI-1605093-VERI-1605094).
- Cisco Systems, Inc.; Single—User Network Access Security TACACS+; Mar. 1996.
- Cisco; Single—User Network Access Security Tacacs+; Mar. 1995.
- Coe et al. D.; Developing and Deploying Corporate Cryptographic Systems; Jul. 1995.
- Communication News; NSA Provides Value-Added Crypto Security; May 1995.
- Communications News; New Product Information; Dec. 1996; (VERI-1606981-VERI-1606983).
- Community Connexion; Mailing list archives; Community ConneXion Announces Stronghold Version 1.2; Community ConneXion, Inc.; Jul. 16, 1996; (CA955577).
- Community Connexion, Inc.; Stronghold Version 1.3 User's Guide; Community Connexion, Inc.; 1996; (CA956585-CA956614).
- Comp.Security.Unix; password encryption (security) over networks; Google Groups; 1994; (VERI-1605917-VERI-1605919).
- Comp.Security.Unix; secure ID cards; which is best?; Google Groups; 1994; (VERI-1605401-VERI-1605404).
- Computumica Secure Networks GmbH; CryptoGuard VPN System, Secured Connections via Shared Infrastructures; 2005.
- Constance, P.; DISA Buys 180,000 Licenses for Navigator; Government Computer News; Jul. 1996.
- Croes, T.; LAN access worlds CONVERGE; Once-competing vendor camps are now borrowing from each other as business and Internet communities find common ground; Oct. 1995.
- CryptoSwift; CryptoSwift Developer Frequently Asked Questions; Mar. 1997.
- CryptoSwift; CryptoSwift Secure Server Accelerator Frequently Asked Questions; Apr. 1997.
- Csinger, Andrew; Letters to the Editor; Certification: Up and Running; (Reprinted from Web Week, vol. 2, Issue 18, Nov. 18, 1996; (CA956617).

# US 8,127,345 B2

Page 6

- Csinger, Andrew; Technology B.C. Application Form; InterSpect Systems Consulting Corp; OpenMed: a secure authentication protocol for health care information transaction; (CA956562-CA956584). CTI; Letter to Roger Loyer with attachment (Electronic Distribution Facility; Response to BayBank Systems—Request for Proposal; Corporate Technologies, Inc.; Feb. 12, 1996; (CA955582-CA955597).
- Curtin, M.; Introduction to Network Security; Mar. 1997.
- Cybermark; CyberMark appoints chairman, CEO; Columbus Business First; Dec. 27, 1996; American City Business Journals Inc.; (VERI-1607123).
- Cybermark; Frees, John; Ceo Graham Sees Cybermark as a “smart” career move; Columbus Business First; Jan. 3, 1997; American City Business Journals Inc. (VERI-1607124-VERI-1607125).
- Cyberstore Systems Inc. et al.; InterMed and OpenMed: Open Systems for Secure Health Care Information Transaction; Mar. 31, 1995; (CA956497-CA9543503).
- Cyberstore Systems Inc. et al.; OpenMed: Open Systems for Secure Health Care Information Transaction; OpenMed Business Plan; Jul. 29, 1995; (CA956469-CA956496).
- Cyberstore; Certification Authority; (CA958518-CA956528).
- Davis, Beth; Digital Certificate Options Offered; TechwebNews; CMP Media Inc.; Jan. 27, 1997; (CA956816).
- Davis, Beth; Security Check—Digital certificates slow to gain users, despite strides; TechwebNews; CMP Media Inc.; Feb. 10, 1997; (CA958615).
- Davis, R.; Network Authentication Tokens; Dec. 1989.
- Defendants’ Joint Invalidity Contentions and Joint Supplemental Answers and Objections to Plaintiff’s Interrogatory 4; Sep. 5, 2006; *Prism Technologies LLC v. Verisign, Inc.*, et al.; Civil Action No. 05-214-JJF.
- Defendants’ Joint Supplemental Invalidity Contentions in Response to Plaintiff’s Interrogatory No. 4; dated Mar. 12, 2007; *Prism Technologies LLC v. Verisign, Inc.*, et al.; Civil Action No. 1:05-cv-00214-JJF.
- Defendants’ Opening Claim Construction Brief with Exhibits; Sep. 22, 2006; *Prism Technologies LLC v. Verisign, Inc.*, et al.; Civil Action No. 05-214-JJF.
- Defendants’ Responsive Claim Construction Brief; Oct. 13, 2006 (public version dated Oct. 17, 2006); *Prism Technologies LLC v. Verisign, Inc.*, et al.; Civil Action No. 05-214-JJF.
- Duffy, J.; Livingston gets Into ‘Net game with new wares; Aug. 1995. E-Mail Responses by various; LDAP for logon?; May 1996; (CA133836-CA133842).
- E-Mail Responses by various; strong authentication questions; May 1996; (CA134275-CA134277).
- Entrust; Curry, Ian; Entrust Technologies; Entrust® Key Management Overview; Apr. 1996, Version 1.4; Entrust Technologies; (VERI-1605756-VERI-1605762).
- Entrust; Entrust Technologies White paper; Implementing Cryptoki Libraries for Entrust®; Jun. 1997; Version 1.2; Entrust Technologies; (VERI-1605386-VERI-1605400).
- Entrust; Entrust Technologies; Team Profiles; Entrust Technologies; (VERI-1605595-VERI-1605599).
- Entrust; Press Release; Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics Announce PICA Crypto-Alliance; Redwood City, Calif.; Oct. 17, 1996; Northern Telecom; (VERI1604986-VERI-1604989).
- Entrust; Press Release; Choro Systems and Northern Telecom (Nortel) Secure Networks Group Sign VAR Agreement; Ottawa, Canada; Aug. 28, 1995; Northern Telecom; (VERI-1604930-VERI-1604932).
- Entrust; Press Release; Cowboys Call on Northern Telecom (Nortel) to Quarterback “Dallas Cowboys Online”; Dallas; Sep. 6, 1996; Northern Telecom; (VERI-1604981-VERI-1604983).
- Entrust; Press Release; Devon Software Corp. Announces Kyberpass The First User Authenticating Firewall to Incorporate Northern Telecom’s (Nortel) Entrust Data Security Software; Ottawa, ON.; Feb. 14, 1996; Northern Telecom; (VERI-1604952-VERI-1604954).
- Entrust; Press Release; Digital Equipment Corporation to Resell Entrust Technologies’ Enterprise Security Products; Ottawa; Apr. 29, 1997; Northern Telecom; (VERI-1605029-VERI-1605031).
- Entrust; Press Release; Entrust Strengthens Data Security for Microsoft Exchange; Philadelphia; Apr. 7, 1997; Northern Telecom; (VERI-1605023-VERI-1605024).
- Entrust; Press Release; Entrust Technologies Demonstrates Interoperability with Multiple Secure E-Mail Products; Philadelphia; Apr. 7, 1997; Northern Telecom; (VERI-1605018-VERI-1605020).
- Entrust; Press Release; Entrust Technologies Launches Partner Program; Ottawa; Jan. 27, 1997; Northern Telecom; (VERI-1605010-VERI-1605014).
- Entrust; Press Release; Entrust Technologies Names John Ryan CEO and Announces Headquarters; Jan. 27, 1997; Northern Telecom; (VERI-1605008-VERI-1605009).
- Entrust; Press Release; Entrust Technologies Now Shipping Entrust/ WebCA and Entrust/ICE; Philadelphia; Apr. 7, 1997; Northern Telecom; (VERI-1605021-VERI-1605022).
- Entrust; Press Release; Entrust Technologies Sweeps Prestigious Awards at NetWorld+Interop; Las Vegas; May 7, 1997; Northern Telecom; (VERI-1605032-VERI-1605034).
- Entrust; Press Release; Entrust Technologies Unveils Entrust/ICE Desktop Encryption Product Jan. 27, 1997; Northern Telecom; (VERI-1605002-VERI-1605003).
- Entrust; Press Release; Entrust Technologies’ 3.0 Offers Users and Network Managers Unmatched Security and Greater Flexibility; Ottawa; Jun. 2, 1997; Northern Telecom; (VERI-1605036-VERI-1605038).
- Entrust; Press Release; Entrust Technologies’ New Toolkit Will Accelerate Deployment of Internet Applications; Ottawa; Apr. 28, 1997; Northern Telecom; (VERI-1605025-VERI-1605028).
- Entrust; Press Release; Entrust wins SCOAP awards of excellence; Ottawa; May 7, 1996; Northern Telecom; (VERI-1604964-VERI-1604967).
- Entrust; Press Release; Entrust® Technologies’ CAST Encryption Algorithm Now Available for Free Commercial and Non-commercial Use; Ottawa; Jan. 24, 1997; Northern Telecom (VERI-1694999-VERI-1605000).
- Entrust; Press Release; Harbinger Chooses Nortel to Provide Security for Electronic Commerce Solutions Entrust-aware Product List Continues to Grow; Chicago, Illinois; May 15, 1996; Northern Telecom; (VERI-1604970-VERI-1604971).
- Entrust; Press Release; Hewlett-Packard to use Nortel’s Data Security Technology; Ottawa; Aug. 27, 1996; Northern Telecom; (VERI-1604979-VERI-1604980).
- Entrust; Press Release; Hewlett-Packard Turns to Nortel For E-Mail Security Solution; San Francisco; Jan. 16, 1996; Northern Telecom; (VERI-1604947-VERI-1604948).
- Entrust; Press Release; IBM Adds Nortel’s Entrust Security software to Its Internet-Commerce Portfolio; Somers, N.Y.; Aug. 1, 1996; Northern Telecom; (VERI-1604974-VERI-1604976).
- Entrust; Press Release; ICL and Nortel Announce Collaboration For Large-Scale Enterprise Network Security X.500 Directory Supports Entrust Security; Anaheim, California; Apr. 29, 1996; Northern Telecom; (VERI-1604955-VERI-1604956).
- Entrust; Press Release; Information Security Corporation and Entrust Technologies Announce SecretAgent to Work with Entrust; Jan. 27, 1997; Northern Telecom; (VERI-1605015-VERI-1605017).
- Entrust; Press Release; JetForm and Entrust Technologies Announce Worldwide Alliance to Provide Advanced Security Solutions for Forms-Based Workflow and Intranet Applications; San Francisco; Jan. 27, 1997; Northern Telecom; (VERI-1605004-VERI-1605007).
- Entrust; Press Release; Limnor Information Systems Management Integrates Nortel Security Services into Nebula Network Management System (NMS); Dec. 20, 1995; Northern Telecom; (VERI-1604944-VERI-1604946).
- Entrust; Press Release; Microsoft selects Northern Telecom’s Entrust network security technology to provide security for Microsoft Exchange Server; Oct. 17, 1994; Nashville, TN; Northern Telecom; (VERI-1604911-VERI-1604912).
- Entrust; Press Release; Nortel (Northern Telecom) forms Entrust Technologies to Focus on Enterprise Security Market; Dallas; Jan. 2, 1997; Northern Telecom; (VERI-1604996-VERI-1694998).
- Entrust; Press Release; Nortel and LJL Enterprises Team to Offer Scalable and Secure E-Mail; Ottawa, Dec. 12, 1995; Northern Telecom; (VERI-1604924-VERI-1604943).

TX0001-0008

## US 8,127,345 B2

Page 7

- Entrust; Press Release; Nortel Endorses S/MIME Specification Company Developing Toolkit for Secure Messaging Applications; Anaheim, California; Apr. 30, 1996; Northern Telecom; (VERI-1604962-VERI-1604963).
- Entrust; Press Release; Nortel introduces Next Generation Software For Secure Data Communications: Entrust 2.0 Designed for Greater Efficiency and Ease of Use; San Francisco; Jan. 16, 1996; Northern Telecom; (VERI-1604949-VERI-1604951).
- Entrust; Press Release; Nortel Issues Demonstration Certificates for Internet Products Free Certificates Enable SSL; San Jose; Apr. 30, 1996; Northern Telecom; (VERI-1604960-VERI-1604961).
- Entrust; Press Release; Nortel Issues Demonstration Certificates Available for Netscape Navigator 3.0; Chicago, Illinois; May 15, 1996; Northern Telecom; (VERI-1604968-VERI-1604969).
- Entrust; Press Release; Nortel Provides Data Security Technology to PayPro Network; Jun. 5, 1996; Northern Telecom (VERI-1604972-VERI-1604973).
- Entrust; Press Release; Nortel Secure Networks Ships Version of Entrust Running on Windows, Macintosh and UNIX Platforms; Scalable Security Software Can be used Worldwide; Ottawa, Ontario; Jul. 31, 1995; Northern Telecom; (VERI-1604928-VERI-1604929).
- Entrust; Press Release; Nortel Security Services Added to TradeWave Internet Solutions; Integrated Security and Public Key Management Now Available from Single Internet Services Vendor; Austin, Texas; Sep. 25, 1995; Northern Telecom; (VERI-1604933-VERI-1604935).
- Entrust; Press Release; Nortel Unveils Next Level of Entrust Software for Secure Data Communications New Certificate Management Features Set Entrust 2.1 Apart; Ottawa, Aug. 19, 1996; Northern Telecom; (VERI-1604977-VERI-1604978).
- Entrust; Press Release; Nortel's Entrust Data Security Software Chosen by Canadian Government to Provide Public-Key Infrastructure; Ottawa; Sep. 16, 1996; Northern Telecom; (VERI-1604984-VERI-1604985).
- Entrust; Press Release; Northern Telecom (Nortel) and Milkyway Networks Introduce Security Solution to Business Internet Users; Ottawa; Nov. 7, 1995; Northern Telecom; (VERI-1604939-VERI-1604941).
- Entrust; Press Release; Northern Telecom (Nortel) and Tandem Sign Agreement Adding Entrust Security Technology to Tandem's Internet Commerce Offering; Ottawa; Nov. 15, 1996; Northern Telecom (VERI-1604994-VERI-1604995).
- Entrust; Press Release; Northern Telecom (Nortel) First in North America to Receive Computer Security Validation: Entrust Certified by U.S. and Canadian Agencies; Baltimore, Md; Oct. 10, 1995; Northern Telecom; (VERI-1604936-VERI-1604938).
- Entrust; Press Release; Northern Telecom (Nortel) Introduces Web-Based Security Software Product Entrust/WebCA Enables Web Session Security; Dallas; Nov. 11, 1996; Northern Telecom; (VERI-1604992-VERI-1604993).
- Entrust; Press Release; Northern Telecom and ZOOMIT Corporation Announce Secure Encryption and Authentication for Windows-Based LAN E-Mail Applications; Mar. 22, 1994; Nashville, Tenn.; Northern Telecom; (VERI-1604908-VERI-1604910).
- Entrust; Press Release; Northern Telecom introduces network security solution to safeguard data privacy and authenticity; Mar. 22, 1994; Washington, D.C.; Northern Telecom; (VERI-1604906-VERI-1604907).
- Entrust; Press Release; Northern Telecom's Entrust Network Security Product to Support National Semiconductor's iPower PersonaCard Hardware Token; Nov. 29, 1994; Boston, Mass.; Northern Telecom; (VERI-1604913-VERI-1604914).
- Entrust; Press Release; NYCE Chooses Nortel's Entrust as Network Security Solution Software; Dallas; Oct. 29, 1996; Northern Telecom; (VERI-1604990-VERI-1604991).
- Entrust; Press Release; Salomon Brothers Chooses Entrust Product Suite as Data Security Solution; New York; May 27, 1997; Northern Telecom; (VERI-1605034-VERI-1605035).
- Entrust; Press Release; Symantec and Nortel Team to Provide Secure Electronic Forms for Enterprises; Anaheim, California; Apr. 29, 1996; Northern Telecom; (VERI-1604957-VERI-1604959).
- Entrust; Press Releases; Control Data adds Nortel (Northern Telecom) Secure Networks' public-key security product to message integration solution; Entrust to provide Mail\*Hub with security services for electronic commerce; New Orleans, LA; May 8, 1995; Northern Telecom; (VERI-1604919-VERI-1604921).
- Entrust; Press Releases; Department of National Defence awards contract to Northern Telecom and ZOOMIT for secure e-mail system; Toronto, Ontario; Mar. 22, 1995; Northern Telecom; (VERI-1604917-VERI-1604918).
- Entrust; Press Releases; New network security system provides private, secure data communications using Nortel's Entrust product; Ottawa, May 15, 1995; Northern Telecom; (VERI-1604925-VERI-1604927).
- Entrust; Press Releases; Northern Telecom licenses security token technology from Chrysalis ITS for hardware extensions to Entrust network security; Redwood Stores, CA; Jan. 9, 1995; Northern Telecom; (VERI-1604915-VERI-1604916).
- Entrust; Press Releases; Shana and Nortel (Northern Telecom) Secure Networks announce Informed's support for Entrust; Collaboration offers authentication for Macintosh and Windows forms; New Orleans, LA; May 8, 1995; Northern Telecom; (VERI-1604922-VERI-1604924).
- European Search Report dated Nov. 3, 2004 of European Application No. 01112859.2; (VERI-1606092-VERI-1606094).
- Federal Computer Week; Advertisement; FCW.Com; (CA955605-CA955606).
- Federal Computer Week; Elizabeth Sikorovsky; Xcert aims to simplify public key infrastructure. (Xcert Software's Sentry Certification Authority data security software) (Product Announcement); vol. 10, Issue 17, Jul. 1, 1996; (CA956511).
- Freier et al.; The SSL Protocol Version 3.0; Mar. 1996.
- Finseth, C.; RFC 1492—An Access Control Protocol, Sometimes Called TACACS; Jul. 1993.
- Fischer International; Smarty; Smarty™ Smart Card Reader; Executive Summary; Fischer International Systems Corporation; 1997; (VERI-1606164-VERI-1606174).
- Ford, Warwick; Computer Communications Security: Principles, Standard Protocols and Techniques; PTR Prentice Hall; 1994; (CA956622-CA957126).
- Franks et al.; RFC 2069—An Extension to HTTP: Digest Access Authentication; Jan. 1997.
- Freier et al.; The SSL Protocol Version 3.0 draft-freier-ssl-version3-02.txt; Nov. 1996.
- Freier et al.; The SSL Protocol Version 3.0, Internet Draft http://wp.netscape.com/eng/ssl3/ssl-toc.html; Mar. 1996.
- Fruth, P.; Product Update: CE Software Quickmail 3.5; Nov. 1995.
- Galvin, Peter; Practicing what I preach: How I set up a secure e-commerce site; Security: Pete's Wicked World; 1997; (CA957611-CA957615).
- Galvin, Peter; Trials and tribulations of building an e-commerce server; Security: Pete's Wicked World; Apr. 1997; (CA955821-CA955828).
- Gaskell et al.; RFC 71.0—improved Security for Smart Card Use in DCE; Open Software Foundation Request For Comments 71.0; Feb. 1995.
- Gasket Integrating Smart Cards into Kerberos; Feb. 2000.
- Gauntlet™ 3.1 for IRIX™ Administrator's Guide for IRIX 5.3; Document No. 007-2826-002; Silicon Graphics, Inc.; 1996; (CA954783-CA955015).
- Gauntlet™3.1.1 for IRIX™ 6.2 Administrator's Guide; Document No. 007-2826-003; Silicon Graphics, Inc.; 1996; (CA955016-CA955263).
- GE Information Services; New Generations of Secure Internet Commerce Unveiled by GE Information Services; GE Information Services; Feb. 6, 1996; (CA955607-CA955609).
- Gifford et al.; Payment Switches for Open Networks; Jul. 1995.
- Gifford et al.; Payment Switches for Open Networks; USENIX Association; New York; Jul. 1995; (CA140714-CA140721).
- Global.H—RSAEURO types and constants; J.S.A. Kapp 1994-1996; (VERI-0015459-VERI-0015460).
- Going Public the IPO Reporter; Securities Data Publishing; 1996; (CA956278-CA956328).
- Goldberg, D.; The Mitre User Authentication System; Aug. 1990.
- Haller, N.; RFC 1704—On Internet Authentication; Oct. 1994.

TX0001-0009

## US 8,127,345 B2

Page 8

- Haller, N.; RFC 1760—The S/Key One-Time Password System; Feb. 1995.
- Harrel, Heather; V-One launches its new federal division; FCW. COM; Mar. 3, 1997; (CA957465-CA-957466).
- Hinnebusch, Mark; Z39.50 Implementors Workshop; Aug. 8, 1996; (CA956529-CA956531).
- Howes et al.; CITI Technical Report 95-7; A Scalable, Deployable Directory Service Framework for the Internet; Jul. 1995.
- Howes et al.; RFC 1823—The LDAP Application Program Interface; Aug. 1995.
- Howes et al.; The LDAP URL Format (Internet Draft); Draft-ietf-asid-ldapv3-url-00.txt; Mar. 1997.
- Howes, T.; An X.500 and LDAP Database: Design and Implementation; Dec. 2003.
- Howes, T.; CITI Technical Report 95-8; The Lightweight Directors Access Protocol: X.500 Lite; Jul. 1995.
- Hunwick, T.; RFC 8.2—Security Requirements for DCE; Aug. 1996.
- IBM; Introduction to DCE; 1996.
- IBM; Presentation at the Securities Industry Middleware Council, re DCE RFC 68.4 Update; Feb. 1999.
- InfoDev-Security.net; Chapter 5. Identification and Authentication; 2003.
- IRE; IRE and CyberGuard Announce Virtual Private Network Security Solution for Enabling Low Cost Internet Business Communication; SafeNet/Enterprise—Enables the Secure Use of Public Networks for Private Business Transactions; Atlanta, GA (Sep. 17, 1996); Information Resource Engineering, Inc.; (VERI-1606027-VERI-1606029).
- IRE; News Release; Dan Mosley Joins IRE Advisory Board; Baltimore, Maryland; Mar. 10, 1997; Information Resource Engineering; (VERI-1605847-VERI-1605848).
- IRE; News Release; Former United States Treasury Secretary to Chair IRE Advisory Board; Baltimore, Maryland; Feb. 5, 1997; Information Resource Engineering; (VERI-1605855-VERI-1605856).
- IRE; News Release; France Telecom's Nexus International Joins IRE to Expand Brazil's Network Security Market; Baltimore, Maryland; Nov. 18, 1997; Information Resource Engineering; (VERI-1605883-VERI-1605884).
- IRE; News Release; Industry Executive Joins IRE to Lead OEM Effort; Interest in Low-Cost SafeNet Technology Results in New Sales Channel; Baltimore, Maryland; Sep. 17, 1997; Information Resource Engineering; (VERI-1605808-VERI-1605809).
- IRE; News Release; Internet Security for the Millennium Available Now; Year 2000 Compliance Makes SafeNet™ the Security Solution for Tomorrow's Electronic Business; Baltimore, Maryland; Dec. 4, 1997; Information Resource Engineering; (VERI-1605845-VERI-1605846).
- IRE; News Release; IRE adds International Sales VP; Baltimore, Maryland; Nov. 12, 1996; Information Resource Engineering; (VERI-1605869).
- IRE; News Release; IRE and Analog Devices to Provide Low-Cost, Secure Communications Chip for Electronic Commerce; Jan. 9, 1997; Information Resource Engineering; (VERI-1605857-VERI-1605859).
- IRE; News Release; IRE and Cyberguard Partner to Provide Complete Security Solution for Internet Business Communication; Aug. 8, 1996; Information Resource Engineering; (VERI-1605880-VERI-1605882).
- IRE; News Release; IRE and Lockheed Martin IS&T Form Strategic Alliance to Offer Turn-Key Secure Electronic Commerce; Jul. 16, 1997; Information Resource Engineering; (VERI-1605817-VERI-1605818).
- IRE; News Release; IRE and MCI Announce Sales and Marketing Agreement for Secure Internet Products and Services; Nov. 14, 1996; Information Resource Engineering; (VERI-1605867-VERI-1605868).
- IRE; News Release; IRE Announces Montgomery Securities as Investment Banking Adviser and Market Maker; Baltimore, Maryland; Jan. 6, 1997; Information Resource Engineering; (VERI-1605862).
- IRE; News Release; IRE Announces New Chief Financial Officer; Baltimore, Maryland; Jul. 21, 1997; Information Resource Engineering; (VERI-1605816).
- IRE; News Release; IRE Debuts SafeNet™ Partner Program, Increases Availability of Industry-Leading Internet Security Solutions; Information Resource Engineering; Baltimore, Maryland; Oct. 21, 1997; (VERI-1605899-VERI-1605900).
- IRE; News Release; IRE Demonstrates Standard Compliant/Public Key Leadership for Internet Virtual Private Networks; Industry test shows SafeNet/Enterprise capable of secure Internet Interoperability; Baltimore, Maryland; Feb. 11, 1997; Information Resource Engineering; (VERI-1605853-VERI-1605854).
- IRE; News Release; IRE Frame Relay Encryptor Makes Business on High Speed Computer Networks a Reality; SafeNet/Frame Currently Showcasing at NetWorld+Interop; Baltimore, Maryland; May 8, 1997; Information Resource Engineering; (VERI-1605827-VERI-1605828).
- IRE; News Release; IRE Introduces Encryption Software for Windows; Baltimore, Maryland; Apr. 24, 1997; Information Resource Engineering; (VERI-1605834-VERI-1605835).
- IRE; News Release; IRE Products to Secure Virtual Banking System in Argentina; Baltimore, Maryland; Aug. 6, 1997; Information Resource Engineering; (VERI-1605814-VERI-1605815).
- IRE; News Release; IRE Receives Patent for Secure Portable Modem; Baltimore, Maryland; Sep. 9, 1996; Information Resource Engineering; (VERI-1605878-VERI-1605879).
- IRE; News Release; IRE Reports 1996 Financial Results; Baltimore, Maryland; Mar. 24, 1997; Information Resource Engineering; (VERI-1605839-VERI-1605840).
- IRE; News Release; IRE Reports Improved Financial Results; Baltimore, Maryland; Mar. 12, 1997; Information Resource Engineering; (VERI-1605825-VERI-1605826).
- IRE; News Release; IRE Reports Strong Financial Growth; Baltimore, Maryland; Aug. 11, 1997; Information Resource Engineering; (VERI-1605812-VERI-1605813).
- IRE; News Release; IRE Reports Third Quarter Results; Baltimore, Maryland; Nov. 14, 1996; Information Resource Engineering; (VERI-1605865-VERI-1605866).
- IRE; News Release; IRE SafeNet Products Protect Consumer Credit Applications on the Internet; Baltimore, Maryland; Sep. 3, 1997; Information Resource Engineering; (VERI-1605810-VERI-1605811).
- IRE; News Release; IRE SafeNet™ Products to Protect GTE's Internet-based Crime Fighting Service; Information Resource Engineering; Baltimore, Maryland; Oct. 29, 1997; (VERI-1605897-VERI-1605898).
- IRE; News Release; IRE ships 3,000<sup>th</sup> SafeNet? Product for secure Intranet use; Baltimore, Maryland; May 23, 1996; Information Resource Engineering; (VERI-1605800-VERI-1605801).
- IRE; News Release; IRE Significantly Expands Distribution in Latin America Adds Eight Major Distribution Channels; Baltimore, Maryland; Jun. 3, 1997; Information Resource Engineering; (VERI-1605819-VERI-1605820).
- IRE; News Release; IRE Smartcard/Readers to be Used in U.S. Treasury Electronic Check Pilot Program; Baltimore, Maryland, Oct. 8, 1997; Information Resource Engineering; (VERI-1605804-VERI-1605805).
- IRE; News Release; IRE Subsidiary Introduces Highly Secure Frame Relay Encryptor for Computer Transmission; Both 128-bit and DES Algorithms Are Offered; Baltimore, Maryland; Mar. 12, 1997; Information Resource Engineering; (VERI-1605843-VERI-1605844).
- IRE; News Release; IRE Subsidiary Wins Contract; Will Secure Swiss Electronic Payment System; Baltimore, Maryland; Nov. 12, 1997; Information Resource Engineering; (VERI-1605893-VERI-1605894).
- IRE; News Release; IRE Takes Lead in Building Secure Foundation for Electronic Commerce on the Internet; Partners with NIST to Develop Public Key Standards; Baltimore, Maryland; Jul. 24, 1996; Information Resource Engineering; (VERI-1605885-VERI-1605886).
- IRE; News Release; IRE to Expand Distribution Channels in the U.S.; Names New Sales Executive to Lead the Development; Balti-

TX0001-0010

- more, Maryland; May 20, 1997; Information Resource Engineering; (VERI-1605823-VERI-1605824).
- IRE; News Release; IRE to Penetrate Japanese Market Through Distribution Agreement with Kanematsu; Baltimore, Maryland; Mar. 31, 1997; Information Resource Engineering; (VERI-1605836-VERI-1605838).
- IRE; News Release; IRE to Product Revolutionary Low-Cost Secure Communications Chip; Baltimore, Maryland; Jan. 9, 1997; Information Resource Engineering; (VERI-1605860-VERI-1605861).
- IRE; News Release; IRE to Showcase Low Cost Smartcard Security Token; Baltimore, Maryland; May 1, 1997; Information Resource Engineering; (VERI-1605832-VERI-1605833).
- IRE; News Release; IRE's Highly Secure Encryption Systems Now Available for Sale Worldwide; Company Receives Export Approval from Commerce Department; Baltimore, Maryland; Mar. 14, 1997; Information Resource Engineering; (VERI-1605841-VERI-1605842).
- IRE; News Release; IRE's Internet Security Center Now On-Line Appoints Dr. Garry Meyer as Managing Director; Baltimore, Maryland; Jul. 11, 1996; Information Resource Engineering; (VERI-1605887-VERI-1605888).
- IRE; News Release; IRE's Internet Security System Chosen as Best of Show Finalist for Interop 1996; Baltimore, Maryland; Sep. 16, 1996; Information Resource Engineering; (VERI-1605821-VERI-1605822).
- IRE; News Release; IRE's MMCI Relationship Likely to Become Marketing Alliance; Baltimore, Maryland; Oct. 18, 1998; Information Resource Engineering; (VERI-1605870-VERI-1605871).
- IRE; News Release; IRE's SafeNet™ Products Achieve Interoperability in Industry Workshop; Baltimore, Maryland, Oct. 15, 1997; Information Resource Engineering; (VERI-1605802-VERI-1605803).
- IRE; News Release; SafeNet Certified as Providing Strongest Security For Internet; New Designation to Give IRE a Competitive Edge; Baltimore, Maryland; Nov. 24, 1997; Information Resource Engineering; (VERI-1605863-VERI-1605864).
- IRE; News Release; State of Maryland Services to Go On-Line Using IRE SafeNet™ Products; Vehicle Registration Among Government Services to be Available on the Internet; Baltimore, Maryland; Sep. 22, 1997; Information Resource Engineering; (VERI-1605806-VERI-1605807).
- IRE; News Release; Strong SafeNet™ Sales Result in Third Quarter Revenue Growth for IRE; Information Resource Engineering; Baltimore, Maryland; Nov. 6, 1997; (VERI-1605895-VERI-1605896).
- IRE; News Release; Sun Microsystems Internet Commerce Group and IRE to Link and Distribute Products for Secure Commerce on the Internet; Apr. 2, 1996; Information Resource Engineering; (VERI-1605891-VERI-1605892).
- IRE; News Release; TRW Purchases IRE Encryption Systems to Protect Treasury communications Nationwide; Baltimore, Maryland; Feb. 13, 1997; Information Resource Engineering; (VERI-1605851-VERI-1605852).
- IRE; News Release; U.S. Robotics and IRE Team to Announce Industry's First Complete Remote Access and Encryption System for Individuals, Enterprises and the Internet; New Strategic Relationship, Including x2, Expected to Accelerate Electronic Commerce and Remote Access Over Internet and Public Networks; May 7, 1997; Information Resource Engineering; (VERI-1605829-VERI-1605831).
- IRE; News Release; U.S. Secret Service Using IRE's Secure Modem During Presidential Campaign; Baltimore, Maryland; Sep. 26, 1996; Information Resource Engineering; (VERI-1605874-VERI-1605875).
- IRE; News Release; U.S. Treasury Renews Contract with IRE for Secure Electronic Commerce System; IRE's Network Security Products in Use Since 1991; Baltimore, Maryland; Oct. 15, 1996; Information Resource Engineering; (VERI-1605872-VERI-1605873).
- IRE; News Release; Vini Cerf to Serve on IRE Advisory Board; Baltimore, Maryland; Feb. 18, 1997; Information Resource Engineering; (VERI-1605849-VERI-1605850).
- ISDN News; Livingston Launches ISDN Router, Too; May 1996.
- ISO/IEC X.509 Information Technology—Open Systems Interconnection—The Directory: Authentication Framework; Nov. 1993.
- Israel et al.; Authentication in Office System Internetworks; ACM Transactions of Office Information Systems; vol. 1, No. 3; Jun. 1983.
- Ito et al.; CITI Technical Report 98-7; Smartcard Integration and Kerberos V5; Dec. 1998.
- ITU-T; Data Networks and Open System Communications Security; Information Technology—Open Systems Interconnection—Security Frameworks for Open Systems: Access Control Framework; ITU-T Recommendation X.812; International Telecommunication Union; 1996; (CA957547-CA957594).
- ITU-T; Data Networks and Open System Communications, Security; Information Technology—Open Systems Interconnection—Security Frameworks for Open Systems: Overview; ITU-T Recommendation X.810; International Telecommunication Union; 1996 (CA957470-CA957495).
- ITU-T; Data Networks and Open System Communications, Security; Information Technology—Open Systems Interconnection—Security Frameworks for Open Systems: Authentication Framework; ITU-T Recommendation X.811; International Telecommunication Union; 1996; (CA957496-CA957546).
- Janson et al.; Safe Single-Sign-On Protocol with Minimal Password Exposure No-Decryption, and Technology-Adaptivity; Mar. 1995.
- Jeffcoat et al.; Internet Security: Strategies and Solutions; Sep. 1997.
- Jones, J.; Securing the World Wide Web: Smart Tokens and Their Implementation; Dec. 1995.
- K. Siau et al.; Xcert Software, Inc.—The Next Step Forward (B); Aug. 1997.
- Kaufman, C.; RFC 1507—DASS, Distributed Authentication Security Service; Sep. 1993.
- Kemp, D.; The Public Key Login Protocol; <draft-kemp-auth-pklogin-01.txt>; Aug. 13, 1996.
- Kemp, D.; The Public Key Login Protocol; <draft-kemp-auth-pklogin-02.txt>; Nov. 26, 1996.
- Kent, Stephen Thomas; Encryption-Based Protection Protocols for Interactive User-Computer Communication Over Physically Unsecured Channels; Massachusetts Institute of Technology; Jun. 1976; (VERI-1605635-VERI-1605755).
- King, C.; Web-Access Authentication Using RADIUS: An Intermediate Method of Secure Exchanges on the Web; Aug. 1996.
- Kohl et al.; RFC 1510—The Kerberos Network Authentication Service (V5); Internet Engineering Task Force; Sep. 1993.
- Kohnfelder; Towards a Practical Public-Key Cryptosystem; May 1978.
- Kotanchik, J.; RFC 59.0—Kerberos and Two-Factor Authentication; Mar. 1994.
- Krajewski, Jr. et al.; Applicability of Smart Cards to Network User Authentication; Computing Systems; vol. 7, No. 1; 1994.
- Lai et al.; Endorsements, Licensing, and Insurance for Distributed System Services; Information Services Institute University of Southern California; Nov. 1994.
- Lennon et al.; Transaction Response Message Authentication (Des/Kp); Dec. 1983.
- Linn, J.; Practical Authentication for Distributed Computing; 1990.
- Linn, J.; RFC 1508—Generic Security Service Application Program Interface; Sep. 1993.
- Livingston Enterprises, Inc.; RADIUS Administrator's Guide; May 1997.
- Livingston Enterprises, Inc.; SecurID Installation; 1996.
- Livingston Enterprises; RADIUS software documents; Livingston Enterprises, Inc.; Dec. 1994-Apr. 1995; (VERI-1606882-VERI-1606980).
- Livingston Enterprises; RADIUS Working Group Internet Draft; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-radius-00.txt; Livingston Enterprises, Inc.; May 1995; (VERI-1607188-VERI-1607257).
- Livingston Enterprises; RADIUS Working Group Internet-Draft; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-radius-01.txt; Livingston Enterprises, Inc.; Nov. 1995; (VERI-1607258-VERI-1607336).
- Livingston Enterprises; RADIUS Working Group Internet-Draft; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-radius-02.txt; Livingston Enterprises, Inc.; May 1996; (VERI-1607337-VERI-1607414).

# US 8,127,345 B2

Page 10

- Livingston Enterprises; RADIUS Working Group Internet-Draft; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-radius-03.txt; Livingston Enterprises, Inc.; May 1996; (VERI-1607415-VERI-1607418).
- Lloyd, B.; RFC 1334—PPP Authentication Protocols; Oct. 1992.
- Looi, M. et al; Enhancing SESAMEV4 with Smart Cards; Sep. 1998.
- Lowry, J.; Location-Independent Information Object Security; IEEE; 1995.
- Lucent Technologies; Radius Code from Lucent radiusd.c; RADIUS, Remove Authentication Dial in User Service; 1992-1999; Lucent Technologies Inc.; pp. 1-48; (VERI-1607419-VERI-1607466).
- McLaughlin; SunWorld News: Directory of the Month of Jun. 1996.
- McLaughlin; SunWorld News: New Products for the Week of May 27; Jun. 1996.
- Memorandum Opinion; Document 448; filed Apr. 2, 2007; *Prism Technologies LLC v. Verisign, Inc.* et al.; Civil Action No. 1:05-cv-00214-JFJ.
- Metzger et al.; RFC 1828—IP Authentication Using Keyed MDS; Aug. 1995.
- Micali, S.; Enhanced Certificate Revocation System; 1995.
- Micali; Efficient Certificate Revocation; Mar. 1996.
- Microsoft; The Microsoft Internet Security Framework: Technology for Secure Communication, Access Control, and Commerce; Dec. 1996.
- Miler, M.; When remote access needs to be blocked; Nov. 14, 1994.
- Mills, D.L.; RFC 1004—A Distributed Protocol Authentication Scheme; Apr. 1987.
- Misc. Activism.Progressive; Horvitz, Robert; NATO support for key-escrow crypto (long); Google Groups; 1995; (VERI-1605777-VERI-1605793).
- Myers et al.; Online Certificate Status Protocol, Version 2; Draft-ietf-pkix-ocspv2-00.txt; Sep. 2000.
- Myers et al.; RFC 2560—X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP; Jun. 1999.
- Myers, J.; RFC 1731—IMAP4 Authentication Mechanisms; Dec. 1994.
- N. Nagaratna et al.; Resource Access Control for an Internet User Agent; Jun. 1997.
- NameFLOW—Paradise—Quarterly Service Report Oct.-Dec. 1995.
- Naor et al.; Certificate Revocation and Certificate Update; Jan. 1998.
- National Bureau of Standards, U.S. Department of Commerce; Federal Information Processing Standards Publication 83: Specification for Guideline on User Authentication Techniques for Computer Network Access Control; 1980.
- National Research Council, Computer Science and Telecommunications Board; Cryptography's Role in Securing the Information Society; 1996.
- National Security Agency; Basic Certification Requirements for FORTEZZA—Enabled Applications Version 1.1; Mar. 1997.
- National Security Agency; FORTEZZA—Certification Requirements for File Protection Applications, Version 1.04; Jan. 1996.
- National Security Agency; FORTEZZA Application Developer's Guide, Version R1.0; Jun. 11, 1996.
- National Security Agency; FORTEZZA Application Implementors Guide for the PCMCIA Based FORTEZZA Cryptologic Card, Version 1.00; Jan. 1995.
- National Security Agency; FORTEZZA Application Implementors Guide for the PCMCIA Based FORTEZZA Cryptologic Card, Revision 1.01; Apr. 6, 1995.
- National Security Agency; FORTEZZA Application implementors Guide for the Fortezza Crypto Card ICD Revision P1.5 and the Fortezza Cryptologic Interface Programmers Guide, Revision 1.52; Mar. 5, 1996.
- National Security Agency; Fortezza Certification Requirements for World Wide Web Clients and Servers; Dec. 1996.
- National Security Agency; FORTEZZA Cryptologic Interface Programmers Guide Revisions 1.52; Jan. 1996.
- National Security Agency; Fortezza Program Overview Version 4.0a; Feb. 1996.
- National Security Agency; Interface Control Document for the Fortezza Crypto Card, Revision P1.5; Dec. 1994.
- National Security Agency; MOSAIC TESSERA document; undated.
- Needham et al.; Using Encryption for Authentication in Computer Networks; Dec. 1978.
- Netegrity; NeTegrity Backgrounder; NeTegrity, Inc.; (CA954733-CA954770).
- Netegrity; NeTegrity Unveils Industry's First Enterprise-Wide, Integrated Network Security Management System; NeTegrity, Inc.; Nov. 15, 1996; (CA9547737-CA954-774).
- Netegrity; NeTegrity Unveils Industry's First Enterprise-Wide, Integrated Network Security Management System; NeTegrity, Inc.; Oct. 15, 1996; (CA954778-CA954777).
- Netegrity; NeTegrity, Inc. and Encotone Ltd. Form U.S. Joint Venture to Market Acoustic Smart Card Technology; NeTegrity, Inc.; Nov. 4, 1996; (CA954771-CA954772).
- Netegrity; Netegrity™ SiteMinder™, Web Agent, Operations Guide for NT Version 2.0; Netegrity, Inc.; 1996-1997; (CA004932-CA004974).
- Netegrity; Netegrity™ SiteMinder™, Web Agent, Operations Guide for NT Version 1.0; Netegrity, Inc.; 1996-1997; (CA005007-CA005012).
- Netegrity; SiteMinder Product/Technology Backgrounder; NeTegrity, Inc.; 1996 (CA954778-CA954780).
- Netegrity; SiteMinder? Authentication Server for Windows NT; NeTegrity, Inc.; 1996; (CA954781-CA954782).
- Netegrity; SiteMinder™ Security Manager; NeTegrity, Inc.; 1996; (CA954775).
- Netegrity; Software & Security: Netegrity's Siteminder software lets net managers get centered on security; NeTegrity, Inc.; Jan. 1997; (CA954730-CA954732).
- Netscape; An Internet Approach to Directories; 1996.
- Netscape; Certificate-Mapping Programmer's Guide; 1997.
- Netscape; FORTEZZA® CryptoSecurity Products; Oct. 1996.
- Netscape; Hitachi and Netscape to Collaborate on Intranet and Extranet Solutions Based on LDAP Standard for Internet Directories; Dec. 1997.
- Netscape; Introduction to Communicator; 1997.
- Netscape; Managing Netscape Servers—Netscape Administration Server 3.0; 1997.
- Netscape; Managing Netscape Servers—Netscape Administration Server 3.0 (online version); 1997.
- Netscape; More Than 40 Companies Join Netscape and U. Michigan to Support Lightweight Directory Access Protocol as Proposed Standard for Internet Directories; Apr. 1996.
- Netscape; Netscape Announces Netscape Certificate Server to Enable Companies to Encrypt Enterprise Communications and Data; Apr. 1996.
- Netscape; Netscape Announces Netscape Suitespot 3.0 for Open Email and Groupware on Intranets; Oct. 1996.
- Netscape; Netscape Certificate Server 1.0—A Powerful Certificate-Management Solution; 1996.
- Netscape; Netscape Certificate Server 1.0 FAQ; 1996.
- Netscape; Netscape Certificate Server Administrator's Guide for Unix; 1997.
- Netscape; Netscape Certificate Server Administrator's Guide for Windows NT; 1997.
- Netscape; Netscape Certificate Server Installation for Unix; 1997.
- Netscape; Netscape Certificate Server Installation for Windows NT; 1997.
- Netscape; Netscape Communicator Supports Smart Cards and Tokens So Mobile Users Can Safely Access Corporate Networks Remotely; Aug. 1997.
- Netscape; Netscape Directory Server 1.0—Server Software for Centralized Directory Management; 1996.
- Netscape; Netscape Directory Server 1.0 Data Sheet; 1996.
- Netscape; Netscape Directory Server 1.0 Fact Sheet; Dec. 1996.
- Netscape; Netscape Directory Server 1.0 FAQ; 1996.
- Netscape; Netscape Enterprise Server 3.0—Administrator's Guide for Windows NT; 1997.
- Netscape; Netscape Enterprise Server 3.0—Administrator's Guide for Unix; 1997.
- Netscape; Netscape Enterprise Server 3.0—The Enterprise-Strength Web Server for the Intranet; 1996.
- Netscape; Netscape Enterprise Server 3.0 FAQ; 1996.

## US 8,127,345 B2

Page 11

- Netscape; Netscape Expands Mission Control to Provide Unified Administration of Intranets and Extranets with Lower Cost of Ownership; Dec. 1997.
- Netscape; Netscape Products With Fortezza Fact Sheet; Feb. 1997.
- Netscape; Netscape SuiteSpot—The Cost-Effective and Full-Service Intranet Solution; 1996.
- Netscape; Netscape SuiteSpot 3.0 FAQ; 1996.
- Netscape; Netscape to Offer Fortezza Cryptographic Capability for Its Software Products; Oct. 1995.
- Netscape; Nsapi Programmer's Guide—Netscape Enterprise Server Version 3.0; 1997.
- Netscape; Securing Communications on the Intranet and Over the Internet; Jul. 1996.
- Netscape; Securing Information Distribution Using Netscape Products with FORTEZZA®; 1996.
- Netscape; Single Sign-On Deployment Guide—Security; 1997.
- Netscape; SSL 2.0 Protocol Specification; Nov. 1994.
- Netscape; the SSL Protocol Version 3.0; Nov. 1996.
- Netscape; U.S. Department of Defense Signs Agreement for Netscape Client and Server Software; Oct. 1997.
- Netscape; Using Netscape with FORTEZZA; 1997.
- Netscape; Web Publisher User's Guide—Netscape Enterprise Server Version 3.0; 1997.
- Netscape; What the Press is Saying About Netscape's New Servers; 1996.
- Network Computing; Certificate Authorities: How Valuable Are They?; Apr. 1, 1997; (CA956512-CA956517).
- Neumann, Peter G.; Architectures and Formal Representations for Secure Systems; Computer Science Laboratory; SRI International EL-243; Oct. 2, 1995; Final Report; SRI Project 6401; (VERI-1605407-VERI-1605564).
- Newman et al.; Kerberos: An Authentication Service for Computer Networks; 1994.
- Newsbytes News Network; GTE's CyberTrust for Web Electronic Commerce; Feb. 6, 1996.
- Newsbytes; UK—Security Dynamics Offers Remote Access Technology; Mar. 1996.
- Oehler et al.; RFC 2085—HMAC-MDS IP Authentication with Replay Prevention; Feb. 1997.
- Open Market, Inc.; Open Market and iCat Strengthen Partnership; PRNewswire; Cambridge, Mass.; Apr. 8; (VERI-1605901-VERI-1605903).
- Open Market, Inc.; Open Market, Interleaf Team on Web "Secure Doc Mgt"; Washingtonpost Newsweek Interactive; Waltham, Massachusetts; Mar. 5, 1996; (VERI-1605905-VERI-1605906).
- Open Market, Inc.; Open Market's "3-Tier Architecture" for Web; Washingtonpost Newsweek Interactive; Waltham, Massachusetts; Mar. 14, 1996; (VERI-1605907-VERI-1605908).
- Oppen et al.; The Clearinghouse a Decentralized Agent for Locating Named Objects in a Distributed Environment; 1983.
- Oracle; Secure Network Services Administrator's Guide Version 2.0; 1995.
- Order; Document 449; filed Apr. 2, 2007; *Prism Technologies LLC v. Verisign, Inc. et al.*; Civil Action No. 1:05-cv-00214-JJF.
- Parekh, Sameer; Re: WWW servers; Community ConneXion, Inc.; Jun. 6, 1996 19:41:26; (CA956618-CA956619).
- Parekh, Sameer; Re: WWW servers; Community ConneXion, Inc.; Jun. 6, 1996 14:21:02; (CA956620-CA956621).
- Parker et al.; Sesame Technology Version 4 Overview; Dec. 1995.
- Pato, J.; RFC 26:0—Using Pre-Authentication to Avoid Password Guessing Attacks; Open Software Foundation Request for Comments 26:0; Jun. 1993.
- Payserv; Tbss (Telematic Base Security Services); Approved procedures and mechanisms for the protection of electronic data communications; IBO 920 353 12.96; Version 1.2; Dec. 6, 1996; (VERI-1606053-VERI-1606091).
- PC Magazine Online; Netscape Shoots to Kill Microsoft and Lotus; Apr. 1996.
- Perkins, C.; RFC 2002—IPMobility Support; Oct. 1996.
- Plaintiff Prism Technologies LLC's Claim Construction Answering Brief; Oct. 13, 2006 with Exhibits; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 05-214-JJF.
- Plaintiff Prism Technologies LLC's Opening Claim Construction Brief and Appendix with Exhibits; Sep. 22, 2006; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 05-214-JJF.
- PR Newswire; Secure Computing Launches Full suite of Products for Enterprise Network Security; Solutions Encompass Perimeter Control, Access Control, Web Browser and Intrawall; Apr. 1996.
- RADIUS server source code; Apr. 1995.
- Rainbow Technologies; IKey 1000 Series Developer's Guide; 2002.
- Rainbow Technologies; Sentinel SuperPro™—Securing the Future of Software Developer's Guide; 1991-1995.
- Rainbow Technologies; SentinelEve3™ Software Protection System Developer's Guide; 1989-1995.
- Rapoza, Jim; Sentry CA cross-checks certificates: Xcert uses LDAP directory secured via SSL for flexible authentication between authorities; PC Week Online; Apr. 16, 1997; (CA956533-CA956535).
- Regents of the University of Michigan; The SLAPD and SLURPD Administrator's Guide, University of Michigan, Release 3.3; Apr. 1996.
- Requests for Comments (RFC) submitted at the *Markman* hearing; Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures and Part II: Certificate-Based Key Management; Feb. 1993.
- Richard, P.; Re: Certificate and CRL's—access and storage; Oct. 1996.
- Richard, P.; Re: LDAP for logon?; May 1996.
- Richard, Patrick C.; E-Mail Responses Re: certificates and CRLs—access and storage; Oct. 15, 1996; (CA134027-CA134028).
- Richard, Patrick; E-Mail Response Re: LDAP for logon?; May 22, 1996; (CA133800-CA133801).
- Richard, Patrick; Re: LDAP for logon?; May 21, 1996; (CA956532).
- Rigney et al.; RADIUS Accounting draft-ietf-radius-accounting-01.txt; Nov. 1995.
- Rigney et al.; RADIUS Accounting; Draft-ietf-radius-accounting-02.txt; Feb. 1996.
- Rigney et al.; RADIUS Accounting; draft-ietf-radius-accounting-03.txt; May 1996.
- Rigney et al.; RADIUS Accounting; draft-ietf-radius-accounting-04.txt; Jun. 1996.
- Rigney et al.; RADIUS Extensions; Draft-ietf-radius-ex-00.txt; Jan. 1997.
- Rigney et al.; RADIUS Extensions; draft-ietf-radius-ext-01.txt; Sep. 1997.
- Rigney et al.; RADIUS Extensions; draft-ietf-radius-ext-02.txt; Oct. 1998.
- Rigney et al.; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-01.txt; Nov. 1995.
- Rigney et al.; Remote Authentication Dial in User Service (RADIUS); draft-ietf-radius-radius-02.txt; Feb. 1996.
- Rigney et al.; Remote Authentication Dial in User Service (RADIUS); draft-ietf-radius-radius-02.txt; May 1996.
- Rigney et al.; Remote Authentication Dial in User Service (RADIUS); Draft-ietf-radius-radius-04.txt; Jun. 1996.
- Rigney et al.; Remote Authentication Dial in User Service (RADIUS); Jan. 1997.
- Rigney et al.; Remote Authentication; Dial in User Service (RADIUS); Apr. 1997.
- Rigney et al.; RFC 2058—Remote Authentication Dial in User Service (RADIUS); Jan. 1997.
- Rigney et al.; RFC 2138—Remote Authentication Dial in User Service (RADIUS); Apr. 1997.
- Rigney; Current Meeting Report; Minutes of the Remote Authentication Dial in User Service ROF (RADIUS); Dec. 1995.
- Rigney; RADIUS Accounting; Jan. 1996.
- Rigney; RADIUS; BayLISA; Mountainview, California; Feb. 1996.
- Rigney; RFC 2139—Radius Accounting; Apr. 1997.
- RISS; Getting Connected; Regional Information Sharing Systems; Jun. 27, 2000; (CA955610-CA955625).
- RISS; Network Fundamentals; Regional Information Sharing Systems; Jun. 26, 2000; (CA955557-CA955573).

- RISSTech; BJS/Search National Conference Justice, E-Government & the Internet Developing Security Policies and Procedures; Regional Information Sharing Systems; Jun. 27, 2000; (CA955648-CA955679).
- RISSTech; Federal CIO Council; XML Community of Practice; RISS/RISSNET Trusted Credential Project; Regional Information Sharing Systems; Feb. 16, 2005; (CA955829-CA955842).
- Rodriguez, K; New TCP/IP Products unveiled at expo; Aug. 1995.
- Rohland, W.S.; Token-Based Information Security for Commercial and Federal Information Networks; Oct. 1995.
- RSA; Baldwin, Robert; Using S/PAY™; Jan. 30, 1997; RSA Data Security, Inc; (VERI-1605920-VERI-1606010).
- RSA; Ciphertext: The RSA Newsletter; vol. 4, No. 1, Spring 1996; RSA Data Security, Inc.; (CA955733-CA955740).
- RSA; S/PAY™; RSA's Developer's Suite for Secure Electronic Transactions (SET); RSA Data Security, Inc.; 1996; (VERI-1606148-VERI-1606151).
- Rubin, A.D.; Independent One-Time Passwords, *Proceedings of the Fifth USENIX UNIX Security Symposium*; Jun. 1995.
- Rubin, Greer, Ranum; A Complete Guide to Web Security Threats and Solutions; 1997.
- Ryan, G.; Making Netscape Compatible with FORTEZZA®—Lessons Learned; Aug. 1999.
- Salz, R.; RFC 100.0—DCE and FORTEZZA; Jan. 1997.
- Salz, R.; RFC 63.3—DCE 1.2 Contents Overview; Oct. 1996.
- Särä, C.; Unified Single Sign-On; Nov. 1998.
- Schneler, B.; Applied Cryptography, 2<sup>nd</sup> ed.; 1996.
- Schroeder, W.; Kerberos/DCE, the Secure Shell, and Practical Internet Security; Oct. 1996.
- Schulz, T.; White Paper: Access Security with SecurID; Nov. 1999.
- Secure Computing Corp; 10-K—for Dec. 31, 1996; Annual Report—Form 10-K; SEC Info; (VERI-1605039-VERI-1605089).
- Secure Computing; internet security; Just How Critical is Data Integrity?; vol. 1, No. 1; Feb. 1997; Secure Computing Corporation; (VERI-1605627-VERI-1605630).
- Secure Computing; internet security; PAYNE, DATA; Elvis spotted?; vol. 1, No. 2, Mar. 1997; Secure Computing Corporation; (VERI-1605631-VERI-1605634).
- Secure Computing; internet security; Victimized company learns a hard lesson vol. 1, No. 3, Apr. 1997; Secure Computing Corporation; (VERI-1605823-VERI-1605626).
- Secure Computing; Lockout™ DES; Client software; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605766-VERI-1605767).
- Secure Computing; Lockout™ DES; Identification and authentication; 1995; Secure Computing Corporation; (VERI-1605772-VERI-1605773).
- Secure Computing; Lockout™ DES; Lockout™ login agent and authentication server; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605768-VERI-1605769).
- Secure Computing; Lockout™ FORTEZZA; Strong Identification and authentication; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605770-VERI-1605771).
- Secure Computing; LOCKOut™ Identification and Authentication; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605606-VERI-1605607).
- Secure Computing; Press Release; Secure Computing Announces Immediate Availability of Sidewinder 3.0; Security Server Employs Fully Integrated Perimeter Security, IPsec Interoperable Encryption, Strong User Authentication, and E-mail Content Filtering; St. Paul, Minn (Sep. 17, 1996); Secure Computing Corporation; (VERI-1606154-VERI-1606155).
- Secure Computing; Secure Computing Demonstration Software; Check out our demos for LOCKOut™ and Sidewinder™; Secure Computing Corporation; 1995; (VERI-1606130).
- Secure Computing; Sidewinder™ Security Server; Apr. 1997; Secure Computing Corporation; (VERI-1606152-VERI-1606153).
- Secure Computing; SNS Deployments; (Last Updated Mar. 17, 1997); Secure Computing Corporation; (VERI-1606175).
- Secure Computing; SNS MLS Solution Set; (Last Updated Mar. 17, 1997); Secure Computing Corporation; (VERI-1606176-VERI-1606177).
- Secure Computing; SNS Product Evolution; (Last Updated Mar. 17, 1997); Secure Computing Corporation; (VERI-1606178-VERI-1606179).
- Secure Computing; SNS support and training services, World class; Secure Computing Corporation offers a variety of Lock® Secure Network Server Installation, Training, and Maintenance programs; 1996; (VERI-1606103-VERI-1606106).
- Secure Computing; What's New?; Secure Computing Corporation; 1996; (VERI-1606156-VERI-1606157).
- Security Dynamics, Inc.; Kerberos and 3<sub>rd</sub> Party Authentication; Mar. 1994.
- Security.itworld.com; Curing Remote—Access Security Ailments; 1996.
- Siau, K.; Xcert Software, Inc.—Abstract; 1999.
- Siebenlist et al.; RFC 68.3—DCE 1.2.2 Public Key Login—Functional Specification; Jan. 1997.
- Siebenlist et al.; RFC 68.4—DCE v.r.m. Public Key Certificate Login—Functional Specification; Apr. 1998.
- Simpson, W.; RFC 1661—The Point -to- Point Protocol (PPP); Jul. 1994.
- Simpson, W.; RFC 1994—PPP Challenge Handshake Authentication Protocol (CHAP); Aug. 1996.
- Smith, C.; LDAP for logon?; May 1996.
- Smith, Sean; Secure Coprocessing Applications and Research Issues; Computer Research and Applications Group (CIC-3); Los Alamos National Laboratory; Los Alamos Unclassified Release LA-UR-96-2805; Aug. 1, 1996; (VERI-1606131-VERI-1606147).
- St. Johns, M.; RFC 912—Authentication Service; Sep. 1984.
- St. Johns, M.; RFC 931—Authentication Server; Sep. 1984.
- Stallings, W.; Mecklermedia's Official Internet World™ Internet Security Handbook; 1995.
- Stefik, M.; Letting Loose the Light: Igniting Commerce in Electronic Publication; 1996.
- Stefik, M.; Trusted Systems; Mar. 1997.
- Stronghold; Community ConneXion announces Stronghold version 1.2; Released: 16<sup>th</sup> Jul. 1996; Red Hat, Inc.; (CA956558-CA956559).
- Stronghold; XCert announces co-marketing agreement to reach largest Internet server market; Released: May 13, 1996; Red Hat, Inc.; (CA956560-CA956561).
- The Open Group; DCE, Distributing Computing Environment Overview; 1996.
- The Open Group; DCE, Distributing Computing Environment, Glossary of Terms; 1996.
- The Open Group; DCE, Distributing Computing Environment, OSF DCE 1.2.2 New Features; 1996.
- The Open Group; Draft Technical Standard, DCE 1.2.3 Public Key Certificate Login (Draft 0.8 for Company Review); Aug. 1998.
- The Open Group; Presentation at the Open Group Member's Meeting re DCE RFC 68.4 Public Key Certificate-Based DCE Login; Apr. 1998.
- The Open Group; Press Release: The Open Group and The Securities Industry Middleware Council Announce Security Solution for Wall Street—*Integrating Smart Cards and DCE*; Jun. 1998.
- The Open Group; Technical Standard DCE 1 Authentication and Security Services; 1997.
- The Open Group; The Open Group Announces General Availability of DCE 1.2.2 with Security and File System Enhancements; 1996.
- TIS; Defense Department Chooses Trusted Information Systems to Provide Network Firewall Plus E-Mail Security; Trusted Information Systems, Inc.; Jul. 10, 1998; (CA955278-CA995279).
- TIS; Firewall Product Functional Summary; NCSA (National Computer Security Association); Trusted Information Systems, Inc.; Jul. 22, 1996; (CA955280-CA955299).
- TIS; Firewall User's Overview; Trusted Information Systems, Inc.; Version dated Feb. 8, 1994; (CA955486-CA955490).
- TIS; Installing the Trusted Information Systems Internet Firewall Toolkit; Marcus J. Ranum; 1997; (CA955300-CA955347).
- TIS; Major Enhancements to Industry-Leading Gauntlet™ Internet Firewall; Trusted Information Systems, Inc.; Jul. 22, 1996; (CA955412-CA955414).
- TIS; Marcus J. Ranum et al.; A Toolkit and Methods for Internet Firewalls; Trusted Information Systems, Inc.; (CA955478-CA955485).

# US 8,127,345 B2

Page 13

- TIS; TIS Firewall Toolkit: Configuration and Administration; Trusted Information Systems, Inc.; Version dated Feb. 17, 1994; (CA955264-CA955277).
- TIS; TIS Firewall Toolkit: Overview; Trusted Information Systems, Inc.; Version dated Jun. 30, 1994; (CA955398-CA955411).
- TIS; TIS Firewall Toolkit; Trusted Information Systems, Inc.; Sep. 1996; (CA955348-CA955397).
- TIS; Trusted information Systems Enhances Industry-Leading Gauntlet™ Internet Firewall; Trusted Information Systems, Inc.; Jan. 23, 1996; (CA955415-CA955417).
- TIS; Trusted Information Systems extends security throughout the network with additions to Gauntlet™ Internet Firewall; Trusted Information Systems, Inc.; Apr. 2, 1996; (CA955418-CA955420).
- TIS; Trusted Information Systems Internet Firewall Toolkit: An Overview; Trusted Information Systems, Inc.; 1993; (CA955421-CA955477).
- Tom Sheldon's Linktionary; FORTEZZA Linktionary entry; Aug. 29, 2006.
- Tung; The Moron's Guide to Kerberos, Version 1.2.2; Jul. 2005.
- Tuvell, W; RFC 98.0—Challenges Concerning Public-Key in DCE; Dec. 1996.
- U.S. Department of Commerce/National Institute of Standards and Technology; FIPS PUB 190—Guideline for the Use of Advanced Authentication Technology Alternatives; Sep. 1994.
- U.S. Department of Commerce; Entity Authentication Using Public Key Cryptography; Feb. 1997.
- U.S. Government; Demonstration Plan for JWID 97; Feb. 1997.
- Udell, Jon; Server and client certificates aren't yet widely used for authentication, but that's changing fast. Here's a progress report.; Web Project.; Digital IDs; Mar. 19, 1997; (CA956461-CA956468).
- V-ONE; The Internet Just Got Real!; Marketing Strategy and Mission; V-ONE Corporation; (CA955549-CA955550).
- V-ONE; "V-ONE Announces SmartWall DMS(TM)" Release DMS/Symposium & Demonstration/V-ONE Information; V-ONE Corporation; Dec. 4, 1996; (CA955694-CA955696).
- V-ONE; Archived News Articles; V-ONE Corporation; (CA955730-CA955732).
- V-ONE; Brian Santo; V-ONE Raises SmartGATE ; (Reprinted from Electronic Engineering TIMES, Dec. 11, 1995); V-ONE Corporation; (CA956273-CA956275).
- V-ONE; CSI Firewall Matrix Search Results; SmartWALL; V-ONE Corporation; (CA95580-CA95581).
- V-ONE; Form S-1/A; V-ONE CORP/DE-VONE, Filed Sep. 6, 1996, Amended Registration statement for face-amount certificate companies; (CA956332-CA956449).
- V-ONE; FORM S-1; V-ONE CORP/DE-VONE, Filed Jun. 21, 1996, General form of registration statement: Initial statement; (CA955843-CA956272).
- V-ONE; Former Spyglass Vice President Joins V-ONE; V-ONE Corporation; 1996; (CA955722-CA955723).
- V-ONE; General Electric Information Services Teams with V-ONE in New Secure Internet Offering; First Deployment of V-ONE's SmartGATE enables the World's Only Smart Card Solution on the Internet; (Reprinted from Business Wire, Feb. 9, 1996); V-ONE Corporation; (CA955574-CA955576).
- V-ONE; General Electric Information Services Teams with V-ONE in New Secure Internet Offering; First Deployment of V-ONE's SmartGATE Enables the World's Only Smart Card Solution on the Internet; (Reprinted from Business Wire, Feb. 9, 1996) V-ONE Corporation; (CA955707-CA955709).
- V-ONE; H?bler; Erick; CyberWallet Offered as Secure Way to Conduct Share Trading On-Line; (Reprinted from SECURITIES Industry Daily, Internet Technology, vol. VII, No. 190, Sep. 29, 1995); V-ONE Corporation; (CA957599-CA957601).
- V-ONE; Internet Firewalls Frequently Asked Questions; V-ONE Corporation; Marcus J. Ranum; 1995; (CA955632-CA955643).
- V-ONE; Karen Rodriguez; New Gateway Verifies Secure Server Link; (Reprinted from Communications Week, Dec. 11, 1995); V-ONE Corporation; (CA955681-CA955682).
- V-ONE; Marcus J. Ranum; Electronic Commerce and Security; V-ONE Corporation; (CA955598-CA955604).
- V-ONE; Marcus Ranum, Father of Firewall Joins V-ONE as Chief Scientist; V-ONE Corporation; 1996; (CA955728-CA955729).
- V-ONE; Marcus Ranum; V-ONE's Security Middleware Product Suite; V-ONE Corporation; (CA956452-CA956458).
- V-ONE; Marjanovic, Steven; Software Beef Up Security of Internet Transactions; (Reprinted from American Banker(R), The Daily Financial Services Newspaper; Friday, Feb. 16, 1996, p. 13); V-ONE Corporation; (CA955551-CA955553).
- V-ONE; Marjanovic, Steven; Software Beef Up Security of Internet Transactions; (Reprinted from American Banker(R), The Daily Financial Services Newspaper; Friday, Feb. 16, 1996, p. 13); V-ONE Corporation; (CA955554-CA955556).
- V-ONE; MCI and V-ONE Corporation Announce Sales Alliance Agreement V-ONE Corporation; Jan. 27, 1997; (CA955714-CA955716).
- V-ONE; New and Noteworthy: A rundown of recent electronic commerce products and services; (Reprinted from Computerworld, Feb. 5, 1996, vol. 30, No. 6); V-ONE Corporation; (CA955578-955579).
- V-ONE; New Network Security Products Spur On-line interest; (Reprinted from Electronic Commerce News (PBI), Mar. 11, 1996); V-ONE Corporation; (CA955644-CA955647).
- V-ONE; Nick Wingfield; V-ONE promises 'net security: SmartGATE client/server tool encrypts across TCP/IP; (Reprinted from INFOWORLD, Internet, Dec. 11, 1995); V-ONE Corporation; (CA955630-CA955631).
- V-ONE; NSA Chooses V-ONE to Protect DMS Networks; (Reprinted from Government Computer News, The National Newspaper of Government Computing, vol. 15, No. 8, Apr. 15, 1998); V-ONE Corporation; (CA955626).
- V-ONE; Paul Merenbloom; SmartGate Internet Security gives good name to middleware: Lan Talk; (Reprinted from INFOWORLD, Feb. 19, 1996); V-ONE Corporation; (CA955627-CA955629).
- V-ONE; Resellers and Distributors; V-ONE Corporation; (CA955816-CA955820).
- V-ONE; Reva Basch; SmartWall Easing Internet Security Concerns; (Reprinted from PCTODAY, Feb. 1996, p. 34); V-ONE Corporation; (CA955683-CA955685).
- V-ONE; Security Middleware: Beyond Firewalls; V-ONE Corporation; Revised: May 23, 1996; (CA955746-CA955747).
- V-ONE; Smartgate: Making networks safe for business, Administrator's Guide; V-ONE Corporation; 1998; (CA957127-CA957480).
- V-ONE; SmartGATE; Secure Connectivity over an Untrusted Network; V-ONE Corporation; Jan. 15, 1996; (CA955810-CA955815).
- V-ONE; SmartGATE™ a product of Security Middleware; V-ONE Corporation; 1996; (CA956276-CA956277).
- V-ONE; SmartWall(TM) to Augment Defense Messaging System: Protecting Highest Military Network; V-ONE Corporation; 1996; (CA955697-CA955698).
- V-ONE; SmartWall(TM) to Augment Defense Messaging System: Protecting Highest Military Network; V-ONE Corporation; 1996; (CA955699-CA955700).
- V-ONE; Success Stories: Regional Law Enforcement Network Reduces Violent Crime While Saving time and Money; Customer Case Study: Regional Law Enforcement Network; V-ONE Corporation; (CA956329-CA956331).
- V-ONE; Trusted Information Systems (TIS) Supports V-ONE's Security Middleware Product SmartGate(TM): TIS to Support SmartGATE Technology in Gauntlet Product Family; V-ONE Corporation; 1996; (CA955718-CA955721).
- V-ONE; V-ONE Announces Business Alliance With Lockheed Martin Federal Systems in Gaithersburg; V-ONE Corporation; Oct. 31, 1996; (CA955688-CA955690).
- V-ONE; V-ONE Announces SmartGate, Enabling Open and Secure Business Transactions on the Internet: New Class of Security Product Allows Businesses to Build a secure Transaction Environment with Existing Legacy or New Client/Server Applications; V-ONE Corporation; Dec. 11, 1995; (CA955691-CA955693).
- V-ONE; V-ONE Announces SmartGate, Enabling Open and Secure Business Transactions on the Internet: New Class of Security Product Allows Businesses to Build a Secure Transaction Environment with Existing Legacy or New Client/Server Applications; V-ONE Corporation; 1996; (CA955701-CA955703).
- V-ONE; V-ONE Announces SmartWall DMS(TM); V-ONE Corporation; Oct. 25, 1996; (CA955686-CA955687).

TX0001-0015

## US 8,127,345 B2

Page 14

- V-ONE; V-ONE Chisels Commerce Drawbridge in Internet Firewalls; (Reprinted from Network Computing, Jan. 15, 1996); V-ONE Corporation; (CA955680).
- V-ONE; V-ONE Corporation Defines a New Class of Security Products: Security Middleware; Industry's First Security Middleware product, SmartGATE, will be demonstrated at RSA Conference in San Francisco; V-ONE Corporation; 1996; (CA955710-CA955713).
- V-ONE; V-ONE launches smart card at FSU; (Reprinted from Online Banking newsletter, Market intelligence for banking executives, vol. 1, Issue 8, Mar. 11, 1996); V-ONE Corporation; (CA955717).
- V-ONE; V-ONE launches smart card at FSU; (Reprinted from Online Banking newsletter, Market intelligence for banking executives, vol. 1, Issue 8, Mar. 11, 2006); V-ONE Corporation; (CA957467).
- V-ONE; V-ONE Leader in Providing Internet Security, Expands Reach Through Agreements with 14 Resellers: VARs Cite Hot Market and Corporate Need for Secure Transactions Via Internet; V-ONE Corporation; Sep. 9; (CA957602-CA957604).
- V-ONE; V-ONE Security for a Connected World; V-ONE Corporation; (CA955491-CA955548).
- V-ONE; V-ONE SmartWall is Best in Infosecurity News Security Supplement; V-ONE Corporation; 1996; (CA955726-CA955727).
- V-ONE; V-ONE to Secure Oracle's Database Network Products; V-ONE Corporation; 1996; (CA955724-CA955725).
- V-ONE; V-ONE, Security Dynamics Announce Technological Interoperability: Security Dynamics' Leading SecurID Authentication Compatible with V-ONE's Top-Ranked Firewall, SmartWall; V-ONE Corporation; 1996; (CA955704-CA955706).
- V-ONE; V-ONE, Software.com, and VNI Partner to Offer First-Of-Its-Kind Secure Messaging: Sender Authentication and Guaranteed Delivery Now Possible Through Post.Office(TM) with SmartGATE(TM); V-ONE Corporation; 1996; (CA957595-CA957598).
- V-ONE; V-ONE's Executive Team; V-ONE Corporation; 1996; (CA956450-CA956451).
- V-ONE; VPN Authentication Encryption Access Control; V-ONE Corporation; (CA955765-CA955809).
- V-ONE; VPN Deployment Lessons Learned; V-ONE Corporation; (CA955748-CA955764).
- Wagner, Mitch; Vanguard makes 'net link with clients (Reprinted from Computer World, vol. 30, No. 8, Feb. 19, 1996); (CA957461-CA957462).
- Wallace, B.; RADIUS to secure remote access; Apr. 1995.
- Warner, M.; RFC 85.0—Improved Public Key Login Protocols for DCE; Oct. 1995.
- Westlaw; (Anonymous); Open Market to acquire Folio Corporation; Information Today; Apr. 1997; ProQuest Info&Learning; (VERI-1605301-VERI-1605302).
- Westlaw; (Anonymous); Open Market unleashes new class of Web software; Information Today; Apr. 1996; ProQuest Info&Learning; (VERI-1605199-VERI-1605202).
- Westlaw; (Anonymous); Retail technology online; Chain Store Age; May 1996; ProQuest Info&Learning; (VERI-1605196-VERI-1605198).
- Westlaw; (Anonymous); Web sheet; Manufacturing Systems; Aug. 1997; ProQuest Info&Learning; (VERI-1605276).
- Westlaw; [Compilation of various articles]; (VERI-1603872-VERI-1603900).
- Westlaw; Adams, Charlotte; Security applications drive government sales (smart cards); Federal Computer Week; Sep. 19, 1994; vol. 8; Issue 28; (VERI-1606804).
- Westlaw; Barnes, Angela; Section: Report on Business; Dow drops 44.83, but Nasdaq raises to record Wall Street puzzled by jobs report; Globe and Mail; Sep. 6, 1997; (VERI-1606833-VERI-1606834).
- Westlaw; Block, Valerie; Florida State U. Smartening Up Its Student IDs; American Banker; Mar. 12, 1996, vol. 161; Issue 48; (VERI-1606762-VERI-1606763).
- Westlaw; Bowen, Ted Smalley; Powersoft hones Internet tool strategy; InfoWorld; Aug. 26, 1996; ProQuest Info&Learning (VERI-1605184-VERI-1605185).
- Westlaw; Bucholtz, Chris; E-entrepreneurs make their mark; Telephony, Internet Edge Supplement; Oct. 6, 1997; ProQuest Info&Learning; (VERI-1605256-VERI-1605259).
- Westlaw; Card Briefs: On-Line Security Eyed for Florida St. ID Tool; American Banker; Jun. 17, 1996; vol. 161; Issue 115; (VERI-1606752).
- Westlaw; Carr, Jim; Users wade through electronic—commerce market; InfoWorld; Jun. 23, 1997; ProQuest Info&Learning; (VERI-1605292-VERI-1605296).
- Westlaw; Chrysalis-ITS Introduces LunaCA; Cryptography System Adds Trust and Assurance to PKI Certification Authority; Sinocast; Nov. 10, 1997; (VERI-1606829-VERI-1606830).
- Westlaw; Cox, John; Cadis brings organization to the Web; Network World; Feb. 10, 1997; ProQuest Info&Learning; (VERI-1605310-VERI-1605311).
- Westlaw; Damore, Kelley; Hardware makers hit the market with server bundles; Computer Reseller News; May 13, 1996; ProQuest Info&Learning; (VERI-1605194-VERI-1605195).
- Westlaw; Darrow, Barbara; Web produces product storm; Computer Reseller News; Dec. 9, 1996; ProQuest Info&Learning; (VERI-1605164-VERI-1605166).
- Westlaw; Davis, Beth; Review Set for Secure Directory Access Spec; Techweb News; Apr. 7, 1997; (VERI-1606866).
- Westlaw; Davis, Jessica; Novell commerce server slides; InfoWorld; Jul. 8, 1996; ProQuest Info&Learning; (VERI-1605189-VERI-1605190).
- Westlaw; Dunlap, Charlotte; Open Market Inks alliance with Portland Software; Computer Reseller News; Aug. 18, 1997; ProQuest Info&Learning; (VERI-1605283-VERI-1605284).
- Westlaw; Dunlap, Charlotte; Open Market woos Web integrators; Computer Reseller News; Aug. 5, 1996; ProQuest Info&Learning; (VERI-1605186-VERI-1605187).
- Westlaw; Edwards, Morris; The electronic commerce Juggernaut; Communications News; Sep. 1997; ProQuest Info&Learning; (VERI-1605262-VERI-1605265).
- Westlaw; Engler, Natalie; The second coming of electronic commerce; Computerworld; Dec. 15, 1997; ProQuest Info&Learning; (VERI-1605229-VERI-1605234).
- Westlaw; Erlanger, Leon; Disarming the Net (security challenges resulting from connection to the Internet) (Network Edition) (Internet/Web/Online Service Information); PC Magazine; Jun. 10, 1997; vol. 16; Issue 11; (VERI-1606856-VERI-1606861).
- Westlaw; Extruded tubing wall thickness; Modern Plastics; May 1986; (VERI-1606812).
- Westlaw; Frank, Diane; The new ROI in point of sale; Datamation; The Gale Group; (VERI-1605776).
- Westlaw; French Payment Developer Puts Banks in the Hot Seat; Bank Technology News; May 1, 1997; (VERI-1606862-VERI-1606864).
- Westlaw; Fulcher, Jim; Shopping made easy; Manufacturing Systems; Oct. 1997; ProQuest Info&Learning; (VERI-1605238-VERI-1605239).
- Westlaw; Geis Using V-ONE SmartGATE; Report on Electronic Commerce; Feb. 20, 1996; vol. 3; Issue 4; (VERI-1606764).
- Westlaw; Gengler, Barbara; V-ONE, Rockville, Md. (SmartGATE secure transaction technology for client/server applications (Product Information) (Brief Article); Internetwork; vol. 7; Issue 4; (VERI-1606760).
- Westlaw; Guenette, David R.; Enterprising information; EMedia Professional; Nov. 1997; ProQuest Info&Learning; (VERI-1605240-VERI-1605251).
- Westlaw; Harrison, Ann; Reach out and buy something; Software Magazine; Apr. 1997; ProQuest Info&Learning; (VERI-1605305-VERI-1605309).
- Westlaw; Hudgins-Bonafield, Christy; Bridging the Business-to-Business Authentication Gap; Network Computing; Jul. 15, 1997; (VERI-1606840-VERI-1606849).
- Westlaw; Hudgins-Bonafield, Christy; Mapping the Rocky Road to Authentication; Network Computing; Jul. 15, 1997; (VERI-1606837-VERI-1606839).
- Westlaw; Hummingbird Does New Java Deal; Newsbytes PM; Sep. 5, 1997; (VERI-1606835).
- Westlaw; Hummingbird Gets Secure Java; ENT; Sep. 24, 1997; (VERI-1606831).

TX0001-0016

- Westlaw; Humphrey, John H. et al.; Comparison tests streamline complex dial-up modem measurements and spring some surprises; Electronic Design; May 1987; vol. 35; (VERI-1606807-VERI-1606811).
- Westlaw; Internet Security & Privacy; V-ONE and Software.com Provide Secure Messaging; Internet Content Report; Jun. 1, 1996; vol. 1; Issue 6; (VERI-1606755).
- Westlaw; Items of Interest; Report on Smart Cards; May 6, 1996; vol. 10; Issue 9; (VERI-1606758-VERI-1606759).
- Westlaw; Java security technology licensed from Xcert Software; Canada StockWatch; Sep. 4, 1997; (VERI-16136836).
- Westlaw; Jones, Chris; iCat and Cadis link online database to Web; InfoWorld; Feb. 10, 1997; ProQuest Info&Learning; (VERI-1605312-VERI-1605313).
- Westlaw; Jones, Chris; OM-Transact connects to invoice and ordering systems; InfoWorld; Dec. 9, 1996; ProQuest Info&Learning; (VERI-1605174-VERI-1605175).
- Westlaw; Jones, Chris; Selling online; InfoWorld; Mar. 17, 1997; ProQuest Info&Learning; (VERI-1605274-VERI-1605275).
- Westlaw; Jones, Chris; SGI will soon deliver virtual-store tools; InfoWorld; Dec. 23/30, 1996; ProQuest Info&Learning; (VERI-1605167-VERI-1605168).
- Westlaw; Jones, Chris; Vendors back SET protocol with product announcements; InfoWorld; Feb. 3, 1997; ProQuest Info&Learning; (VERI-1805314-VERI-1605315).
- Westlaw; Key Management System; Entrust; Network Computing; May 1, 1997; (VERI-1606865).
- Westlaw; Kohlhepp, Robert J.; Securing Intranet Data With SSL Client Certificates; Network Computing; Jul. 1, 1997; (VERI-1606852-VERI-1606855).
- Westlaw; Krill, Paul; Novell to adopt Java, ActiveX architectures; InfoWorld; Mar. 25, 1996; ProQuest Info&Learning; (VERI-1605208-VERI-1605210).
- Westlaw; Kruger, Peter; The net takes its toll; Communications International; May 1996; ProQuest Info&Learning; (VERI-1605191-VERI-1605193).
- Westlaw; Kutler, Jeffrey; Vendors Ready—and Waiting—for E-commerce; American Banker; Feb. 2, 1996; vol. 161; Issue 22; (VERI-1606767-VERI-1606769).
- Westlaw; Kutler, Jeffrey; Card Groups Join Electronic Commerce Initiatives Gemplus a Founding Member of Electronic Business Co-op; American Banker; Jun. 12, 1995; vol. 160; Issue 111; (VERI-1606798-VERI-1606799).
- Westlaw; Lawton, George; Surf's up! The Internet is here. (part 1) (Includes related article); Telephony; Jul. 17, 1995; vol. 229; Issue 3; (VERI-1606788-VERI-1606793).
- Westlaw; Lewis, Peter H.; Internet Commerce: Hold the Anchovies; New York Times; Apr. 7, 1995; (VERI-1606800-VERI-1606801).
- Westlaw; Maddox, Kate; New Net options for business; Informationweek; Mar. 4, 1998; ProQuest Info&Learning; (VERI-1605213).
- Westlaw; Making Net Management Easier; Sinocast; Dec. 22, 1997; (VERI-1608827-VERI-1606828).
- Westlaw; Masud, Sam; iCat signs 120 VARs, Ingram Micro; computer Reseller News; Jan. 13, 1997; ProQuest Info&Learning; (VERI-1605316-VERI-1605317).
- Westlaw; Masud, Sam; OpenMarket hopes to cash in on electronic commerce; Computer Reseller News; Oct. 28, 1996; ProQuest Info & Learning; (VERI-1605178-VERI-1605179).
- Westlaw; Messmer, Ellen et al.; Holiday networking extravaganza on tap; Network World; Dec. 9, 1996; ProQuest Info&Learning; (VERI-1605160-VERI-1605163).
- Westlaw; Messmer, Ellen; Open Market software separates Web content, transaction management; Network World; Mar. 11, 1996; ProQuest Info&Learning; (VERI-1605206-VERI-1605207).
- Westlaw; Messmer, Ellen; Start-up's service dodges Net sales tax; Network World; Jun. 30, 1997; ProQuest Info&Learning; (VERI-1605297-VERI-1605298).
- Westlaw; Michel, Roberto; The Net benefits; Manufacturing Systems; Feb. 1997; ProQuest Info&Learning; (VERI-1605277-VERI-1605282).
- Westlaw; Millman, Howard; Profit ploys for increased income; InfoWorld; Nov. 3, 1997; ProQuest Info&Learning; (VERI-1605235-VERI-1605237).
- Westlaw; Mohan, Suruchi; Effective Internet commerce to hinge on directors; InfoWorld; Sep. 8, 1997; ProQuest Info&Learning; (VERI-1605266-VERI-1605270).
- Westlaw; Murphy, Brian; Telecommunications talk; magazines online, new bulletin boards; and new products; Creative Computing; Jan. 1985; vol. 11; (VERI-1606813-VERI-1606816).
- Westlaw; Nash, Kim S.; Open Market aids Web site upkeep; Computerworld; Mar. 11, 1996; ProQuest Info&Learning; (VERI-1605211-VERI-1605212).
- Westlaw; New Products; Defense Daily; Sep. 15, 1997; vol. 2; (VERI-1606832).
- Westlaw; New Security Technology Products; Security Technology News; Aug. 26, 1994; vol. 2; Issue 17; (VERI-1606805).
- Westlaw; Newing, Rod; A new computing architecture is coming; Management Accounting-London; Dec. 1996; ProQuest Info& Learning; (VERI-1605169-VERI-1605173).
- Westlaw; Online; Report on Electronic Commerce; Apr. 30, 1996; vol. 3; Issue 9; (VERI-1606876-VERI-1606877).
- Westlaw; Orenstein, Alison F.; Banks help merchants tap Internet 'sales floor'; Bank Systems & Technology; Apr. 1997; ProQuest Info&Learning; (VERI-1605303-VERI-1605304).
- Westlaw; Ostertag, Krista; Tightening the Web, fixing the holes; Varbusness; Apr. 1, 1996; (VERI-1606761).
- Westlaw; Pappalardo, Denise; ISPs dress up Web hosting services; Network World; Jul. 28, 1997; ProQuest Info&Learning; (VERI-1605290-VERI-1605291).
- Westlaw; Personnel Roundup; Newsbytes PM; Oct. 13, 1995; (VERI-1606783-VERI-1606784).
- Westlaw; Poole, Jackie; Commerce-enabled sites from ANS; InfoWorld; Jul. 21, 1997; ProQuest Info&Learning; (VERI-1605288-VERI-1605289).
- Westlaw; Premenos and Open Market Announce Strategic OEM Alliance; PR Newswire; Mar. 4, 1996; The Gale Group; (VERI-1605774-VERI-1605775).
- Westlaw; Prince, Cheryl J.; building an Internet payments franchise; Bank Systems & Technology; Sep. 1996; ProQuest Info&Learning; (VERI-1605182-VERI-1605183).
- Westlaw; Reuters, Jennifer Genevieve; Section: Business; IPOS Looked Golden in '95; Memphis Commercial Appeal; Memphis, TN; Jan. 2, 1996; (VERI-1606771-VERI-1606772).
- Westlaw; Reuters; Section: Business; Tech Talk; St. Louis Post-Dispatch; Dec. 13, 1995; (VERI-1606773).
- Westlaw; Rodriguez, Karen; Open market targets business; CommunicationsWeek; Mar. 11, 1996; ProQuest Info&Learning; (VERI-1605203).
- Westlaw; Schmidt, Karen; Section: Metro Hartford; Putting a High-Tech Spin on Computer-Aided Design in Newington; Hartford Courant; Sep. 21, 1995; (VERI-1606785-VERI-1606786).
- Westlaw; Section: Business; ACME Sets Agreement to Market Power Unit; Buffalo News; Feb. 22, 1993; (VERI-1606806).
- Westlaw; Section: Business; Financing Deal; Hartford Courant; Aug. 26, 1995; (VERI-1606787).
- Westlaw; Section: Financial; BioWhittaker Posts 62% Gain in profits for 4<sup>th</sup> Quarter; Baltimore Sun; Dec. 12, 1995; (VERI-1606774-VERI-1606776).
- Westlaw; Section: Financial; MD. Software Product Offers Internet Security; Baltimore Sun; Dec. 9, 1995; (VERI-1606779).
- Westlaw; Section: Financial; Phone Users Can Join in Testing a Speedier Data-Send Service; Baltimore Sun; Oct. 31, 1995 (VERI-1606780-VERI-1606782).
- Westlaw; Spyglass offers software tailoring Mosaic for use by business on the Internet; Software Industry Report; Dec. 19, 1994; vol. 26; issue 24; (VERI-1608802-VERI-1606803).
- Westlaw; Symoens, Jeff; Integration Is key to Commerce; InfoWorld; Oct. 13, 1997; ProQuest Info&Learning; (VERI-1605254-VERI-1605255).
- Westlaw; Symoens, Jeff; Transact 3.0: Scalable solution; InfoWorld; Sep. 8, 1997; ProQuest Info&Learning; (VERI-1605271-VERI-1605273).

- Westlaw; Technology: Crackdown on Internet security; Financial Times Mandate; May 30, 1996; (VERI-1606756).
- Westlaw; Tenderly (No Page); Jul. 14, 1995; (VERI-1606794).
- Westlaw; UK-London: computerized human resource information system (With participation by GATT countries); Tenders Electronic Daily; Jul. 14, 1995; (VERI-1606795-VERI-1606797).
- Westlaw; VeriSign Announces New Partners; Report on Smart Cards; May 6, 1996, vol. 10; Issue 9; (VERI-1606757).
- Westlaw; Virtual Open Network Environment Corp.; Going Public; Aug. 19, 1996; vol. 20; Issue 34; Securities Data Publishing; (VERI-1606750-VERI-1606751).
- Westlaw; V-ONE Securing Payments with Enhanced Firewalls; Retail Delivery News; Jun. 7, 1996; vol. 1; Issue 12; (VERI-1606753-VERI-1606754).
- Westlaw; Wagner, Mitch; Open Market upgrade will support big business on 'net; Computerworld; Dec. 9, 1996; ProQuest Info& Learning; (VERI-1605176-VERI-1605177).
- Westlaw; Wagner, Mitch; Start-up will outsource 'net transactions; Computerworld; Jun. 30, 1997; ProQuest Info& Learning; (VERI-1605299-VERI-1605300).
- Westlaw; Walsh, Jeff; Open Market announces SiteDirector 4.1; InfoWorld; Dec. 15, 1997; ProQuest Info& Learning; (VERI-1605227-VERI-1605228).
- Westlaw; Wexler, Joanie; AT&T rounds out E-commerce line; Network World; Oct. 14, 1998; ProQuest Info& Learning; (VERI-1605180-VERI-1605181).
- Westlaw; Who's who in the CA market; Network Computing; Jul. 15, 1997; (VERI-1606850-VERI-1606851).
- Westlaw; Wilder, Clinton et al.; Pushing outside the enterprise; Informationweek; Aug. 4, 1997; ProQuest Info (VERI-1605285-VERI-1605287).
- Westlaw; Wilder, Clinton et al.; Trusting the Net; Informationweek; Oct. 14, 1996; ProQuest Info& Learning; (VERI-1605156-VERI-1605159).
- Westlaw; Wilder, Clinton; Distributors get their own shot at Web sales; Informationweek; Sep. 8, 1997; ProQuest Info& Learning; (VERI-1605260-VERI-1605261).
- Westlaw; Wilder, Clinton; E-commerce gets real; Informationweek; Dec. 9, 1996; ProQuest Info& Learning; (VERI-1605153-VERI-1605155).
- Westlaw; Wilder, Clinton; E-commerce hosting services to expand; Informationweek; Jul. 22, 1996; ProQuest Info& Learning; (VERI-1605188).
- Westlaw; Wilder, Clinton; Focus on e-commerce; informationweek; Oct. 6, 1997; ProQuest Info (VERI-1605252-VERI-1605253).
- Westlaw; Willett, Shawn; Novell to license Java, build online tools; Computer Reseller News; Mar. 18, 1996; ProQuest Info& Learning; (VERI-1605204-VERI-1605205).
- Westlaw; Wilson, Donald C.; Highest and best use: Preservation use of environmentally significant real estate; Appraisal Journal; Jan. 1996; ProQuest Info& Learning; (VERI-1605214-VERI-1605226).
- Westlaw; Wilson, Donald C.; The principle of rank substitution; Appraisal Journal; Jan. 1997; ProQuest Info (VERI-1605318-VERI-1605331).
- Wirbel, L.; Management platforms, virtual lans shine at showNetWorld; gains aplenty; Apr. 1996.
- Woo et al.; Authentication for Distributed Systems; Jan. 1992.
- Wood, B.; A Case for Avoiding Security-Enhanced HTTP Tools to Improve Security for Web-Based Applications; Feb. 1996.
- Workshop on Network and Distributed Systems Security; Smart Card Augmentation of Kerberos; 1993.
- Workshop on Network and Distributed Systems; An Overview of the Advances SmartCard Access Control System; 1993.
- Workshop on Network and Distributed Systems; Issues Surrounding the Use of Cryptographic Algorithms and Smart Card Applications; 1993.
- Wu; Remote Access Technology; Evaluating the Options; Jul. 1994.
- Xcert Software, Inc.; Excerpt from website Xcert Software, Inc. "Can YOU get through this door?"; 1996.
- Xcert; Can You get through this door?; Xcert YOUR Authority; Xcert Software Inc.; 1996; (CA957468-CA957469).
- Xcert; Fischer International Systems Corporation and Xcert Software Inc demonstrate the first web-based Certificate Authority to interoperate with hardware tokens; Xcert International Inc.; Nov. 12, 1996; (CA956555-CA956557).
- Xcert; Keng Siau et al.; Xcert Software Inc.—The Next Step Forward (B); 1997; (CA142771-CA142777).
- Xcert; Keng Siau; Xcert Software, Inc. Abstract; 1999; (VERI-0235357-VERI-0235382).
- Xcert; Network Computing Magazine Names Xcert's Sentry CA as 'Well-Connected' Award Nominee; Xcert International Inc.; Mar. 7, 1997; (CA956551-CA956552).
- Xcert; Sales FAQ (Frequently Asked Questions); Corporate and Product Overview; Xcert Software, Inc.; 1996-1997; (CA956507-CA956510).
- Xcert; Sales FAQ(Frequently Asked Questions); Download and Support; Xcert Software, Inc.; (CA956504-CA956506).
- Xcert; Sentry CA (Certificate Authority); 1996.
- Xcert; Sentry CA(Certificate Authority); Internet Security Technologies; Xcert International Inc.; 1997; (CA957605-CA957610).
- Xcert; Sentry CA Cross-Checks Certificates, *PC Week Online*; Apr. 1997.
- Xcert; Software Sentry News Media Backgrounder; Xcert International Inc.; Apr. 17, 1996; (CA956536-CA956538).
- Xcert; Software Sentry Technology Announcement; Xcert International Inc.; Apr. 18, 1996; (CA956539-CA956541).
- Xcert; The Xcert Sentry Access Control List Module; (CA137969-CA137972).
- Xcert; The Xcert Sentry Access Control List Module; 1996.
- Xcert; Xcert Announces Co-Marketing Agreement to Reach Largest Internet Server Market; Xcert International Inc.; May 14, 1996; (CA956553-CA956554).
- Xcert; Xcert Software Announces Support for Litronic NetSign™; Xcert International Inc.; Jun. 11, 1997; (CA956545-CA956546).
- Xcert; Xcert Software Inc., Questions and Answers; 1996.
- Xcert; Xcert Software Inc.; /html-docs; Xcert Software Inc.; 1996; (VERI-1605090).
- Xcert; Xcert Software is First to Demonstrate Certification Authority (CA) Interoperability; Xcert International Inc.; Mar. 21, 1997; (CA956550).
- Xcert; Xcert Software, Inc. Questions & Answers; (CA137960-CA137968).
- Xcert; Xcert Software's Certification Authority and Access Control Technology Provides Privacy on Public Networks; Xcert International, Inc.; Jan. 27, 1997; (CA956542-CA956544).
- Xcert; Xcert YOUR Authority; Can YOU get through this door?; Xcert Software Inc.; 1996-1997; (CA957463-CA957464).
- Xcert; Xcert's New Certification Authority and Access Control Technology Offers Unprecedented Safeguards for Electronic Commerce and Communications; Xcert International Inc.; Jun. 24, 1998; (CA956547-CA956549).
- Xcert; Xuda Specification; Xcert Software, Inc.; (CA956459-CA956460).
- Xcert; Xuda Specification; Xcert Software, Inc.; (VERI-1605335-VERI-1605337).
- Xcert; Xuda; Xcert Universal Database API; 1996.
- Xcert; Xuda; Xcert Universal Database API; Internet Security Technologies; Xcert International Inc.; (CA957616-CA957617).
- Yeong et al.; RFC 1777—Lightweight Directory Access Protocol; Mar. 1995.
- Ylönen, T.; SSH—Secure Login Connections Over the Internet; Jul. 1996.
- ZBORAY, Michael R.; Securing Legacy TCP/IP Applications; Gartner, Inc.; ID No. SPA-AUZ-024; Dec. 28, 1995; (CA955741-CA955745).
- Zhong, Q.; Providing Secure Environments for Untrusted Network Applications; 1997.
- Zisman, A.; Business in Vancouver High Tech Office column; May 1996.
- Zisman, Alan; Local software products helping to blaze the way to secure business dealings on the Internet; Business in Vancouver; Issue #342; May 14, 1996; (CA133828-CA133829).
- SiteMinder v. 1.0*; Netegrity, Inc.; 1996-1997.

# US 8,127,345 B2

Page 17

*Prism Technologies LLC, v. Verisign, Inc. et al.; Civil Action No. 05-214 JJF; Plaintiff Prism Technologies LLC's Objections and Responses to Defendant Netegrity, Inc.'s First Set of Interrogatories (Nos. 1-5); Oct. 24, 2005; 18 pages.*

*Prism Technologies LLC, v. Research in Motion, LTD.; Case No. 8:08-cv-00537; Second Amended Answer and Counterclaim of Defendant Research in Motion, Ltd.; Apr. 29, 2010; 28 pages.*

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Declaration of Charles J. Hawkins: (1) In Support of Motion of Complainant Prism Technologies LLC for 45-Day Stay of the Proceedings and Shortened Response Period Hereto; and (2) In Opposition to Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; 6 pages; Exhibit A, 2 pages; Exhibit B, 3 pages; Exhibit C, 2 pages; Exhibit E, 2 pages; Exhibit F, 7 pages; Exhibit G, 13 pages; Exhibit H, 16 pages; Exhibit I, 5 pages; Exhibit J, 10 pages; Exhibit K, 6 pages; Exhibit L, 17 pages; Exhibit M, 62 pages; Exhibit N, 6 pages; Exhibit R, 4 pages; Exhibit T, 53 pages; Apr. 12, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent 7,290,288, Motion; 30 pages; Apr. 12, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Prism Technologies, LLC's Response to RIM's Statement of Material Facts for Which There Is No Genuine Issue; 17 pages; Apr. 12, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Motion of Respondents Research in Motion Limited and Research in Motion Corporation to File a Reply to Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent No. 7,290,288; 4 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Memorandum in Support of Motion of Respondents Research in Motion Limited and Research in Motion Corporation to File a Reply to Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent No. 7,290,288; 3 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; RIM's Reply to Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent No. 7,290,288; Redacted Version; 11 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; RIM's Response to Prism Technologies, LLC's Statement of Material Facts; 13 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Respondents' Research in Motion Limited and Research in Motion Corporation Opposition to Complainant Prism Technologies LLC's Motion for 45-Day Stay of the Proceedings (Motion No. 697-012); Redacted Version; 18 pages; Apr. 22, 2010.

Request for Ex Parte Reexamination of U.S. Patent No. 7,290,288, dated Apr. 8, 2010; pp. 1-288; Exhibit AA, 7 pages; Exhibit L, 43 pages; Exhibit M, 54 pages; Exhibit N, 84 pages; Exhibit O, 63 pages; Exhibit P, 41 pages; Exhibit Q, 29 pages; Exhibit R, 14 pages; Exhibit S, 13 pages; Exhibit T, 13 pages.

Andrews, Whit; Content Sites Vexed By Password Abuse; Reprinted from Web Week, vol. 3, Issue 4; Feb. 17, 1997; 3 pages.

Andrews, Whit; out with the old . . . ; Old Guard of Content Providers Adopt to the Web; Reprinted from Web Week, vol. 2, Issue 20; Dec. 16, 1996; 3 pages.

Bowen, Barry D.; How Popular Sites Use Cookie Technology; Shopping baskets are a natural use for cookies, but uncovered several surprising uses, too; Netscape World; Apr. 1997; 13 pages.

de Laat, C., et al.; Generic AAA Architecture; Request for Comments: 2903; Aug. 2000; 26 pages.

EMV '96; Chip Electronic Commerce Specification, Version 1.0; Dec. 1999; 69 pages.

Farrell, S., et al.; AAA Authorization Requirements; Request for Comments: 2906; Aug. 2000; 23 pages.

OASIS; Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 47 pages.

OASIS; Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 31 pages.

OASIS; Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 23 pages.

OASIS; Glossary for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 13 pages.

OASIS; Security and Privacy Consideration for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 26 pages.

SET Secure Electronic Transaction Specification; Book 1: Business Description; Version 1.0; May 31, 1997; 80 pages.

SET Secure Electronic Transaction Specification; Book 3: Formal Protocol Definition; Version 1.0; May 31, 1997; 251 pages.

SET Secure Electronic Transactions Website Archive; <http://web.archive.org/web/19981206111521/http://www.setco.org/>; Dec. 6, 1998; 1 page.

SET; External Interface Guide to SET Secure Electronic Transaction; Sep. 24, 1997; 118 pages.

Vollbrecht, J., et al.; AAA Authorization Application Examples; Request for Comments: 2905; Aug. 2000; 53 pages.

Vollbrecht, J., et al.; AAA Authorization Framework; Request for Comments: 2904; Aug. 2000; 36 pages.

Defendants' Joint Invalidity Contentions and Joint Supplemental Answer and Objections to Plaintiff's Interrogatory No. 4; *Prism Technologies LLC v. Verisign, Inc.*, et al.; Civil Action No. 05-214-JJF; Sep. 5, 2006; 118 pages.

Defendants' Joint Supplemental Invalidity Contentions in Response to Plaintiff's Interrogatory No. 4; *Prism Technologies LLC v. Verisign, Inc.*, et al.; Civil Action No. 1:05-cv-00214-JJF; dated Mar. 12, 2007; 269 pages.

Defendant Symantec Corp.'s Answer, Affirmative Defenses, and Counterclaims; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-CV-220; Doc. No. 107; filed Aug. 23, 2010; 13 pages. Defendant Autodesk, Inc.'s Answer and Counterclaims; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-Cv-220; Doc. no. 108; filed Aug. 23, 2010; 12 pp.

Defendant Sage Software, Inc.'s Answer to Prism's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-CV-220; Doc. No. 113; filed Sep. 1, 2010; 11 pages.

Defendant Nuance, Inc.'s Answer and Counterclaims; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-CV-220; Doc. No. 119; filed Sep. 7, 2010; 34 pages.

Defendant National Instruments Corp.'s Answer and Counterclaims to Plaintiff's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-CV-220; Doc. No. 120; filed Sep. 7, 2010; 12 pages.

Answer and Counterclaims of Defendant Trend Micro Incorporated to Plaintiff Prism Technologies, LLC's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-CV-220; Doc. No. 121; filed Sep. 7, 2010; 14 pages.

Defendant Adobe Systems Inc.'s Answer and Counterclaims to Plaintiff's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-CV-220; Doc. No. 123; filed Sep. 7, 2010; 13 pages.

Defendant Quark, Inc.'s Answer and Counterclaims to Prism Technologies LLC's Complaint; *Prism Technologies LLC v. Adobe Systems Inc.*, et al.; Case No. 8:10-CV-220; Doc. No. 124; filed Sep. 7, 2010; 11 pages.

TX0001-0019

**US 8,127,345 B2**

Page 18

---

Defendant McAfee, Inc.'s Answer and Counterclaim to Prism's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 131; filed Sep. 10, 2010; 11 pages.

Defendant The Mathworks, Inc.'s First Amended Answer and Counterclaim to Prism's Complaint for Patent Infringement; *Prism Tech-*

*nologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 133; filed Sep. 13, 2010; 11 pages.

Rainbow Technologies; iKey 1000 Series Product Brief; Rev. 1.1; Apr. 27, 2001.

\* cited by examiner

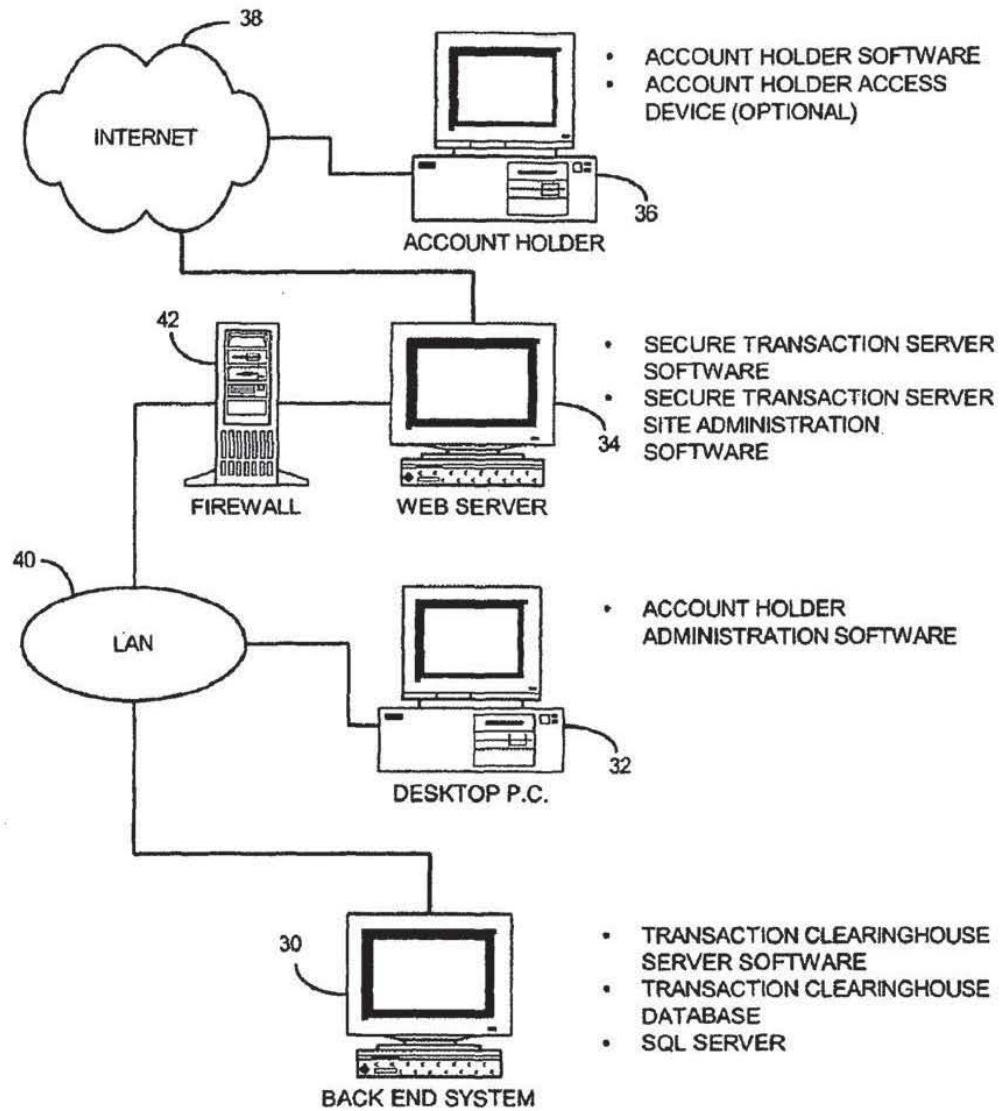


FIG. 1

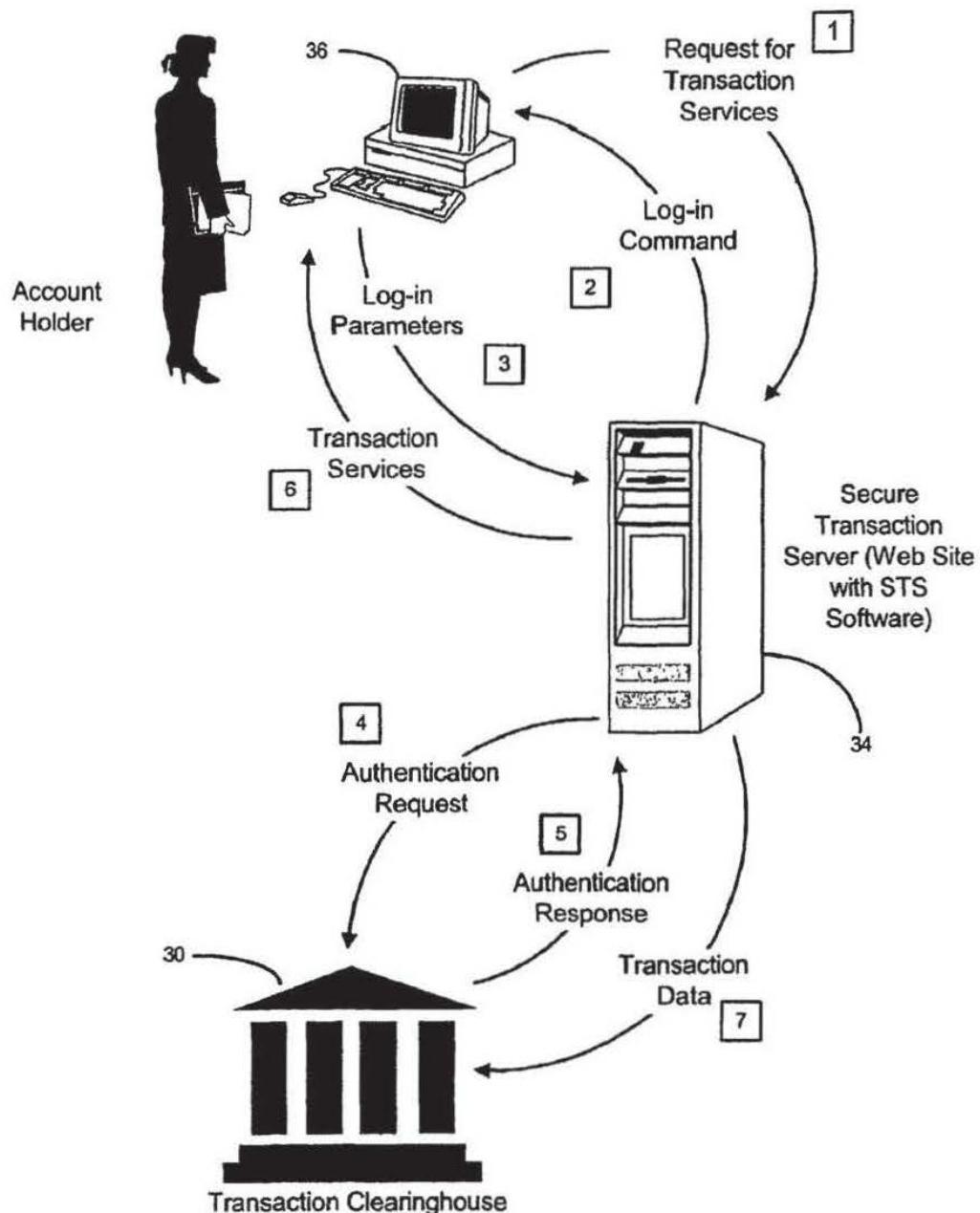


FIG. 2

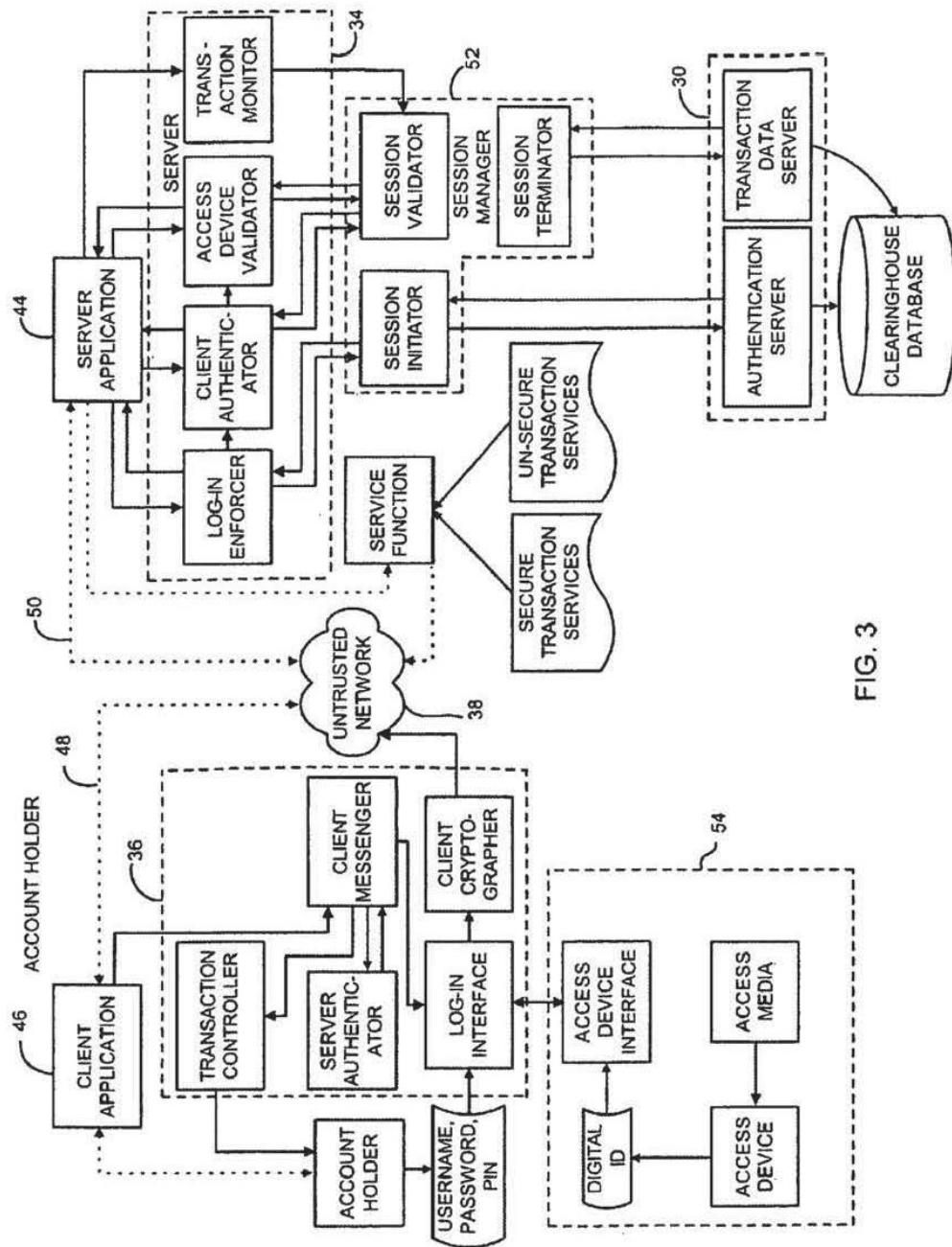
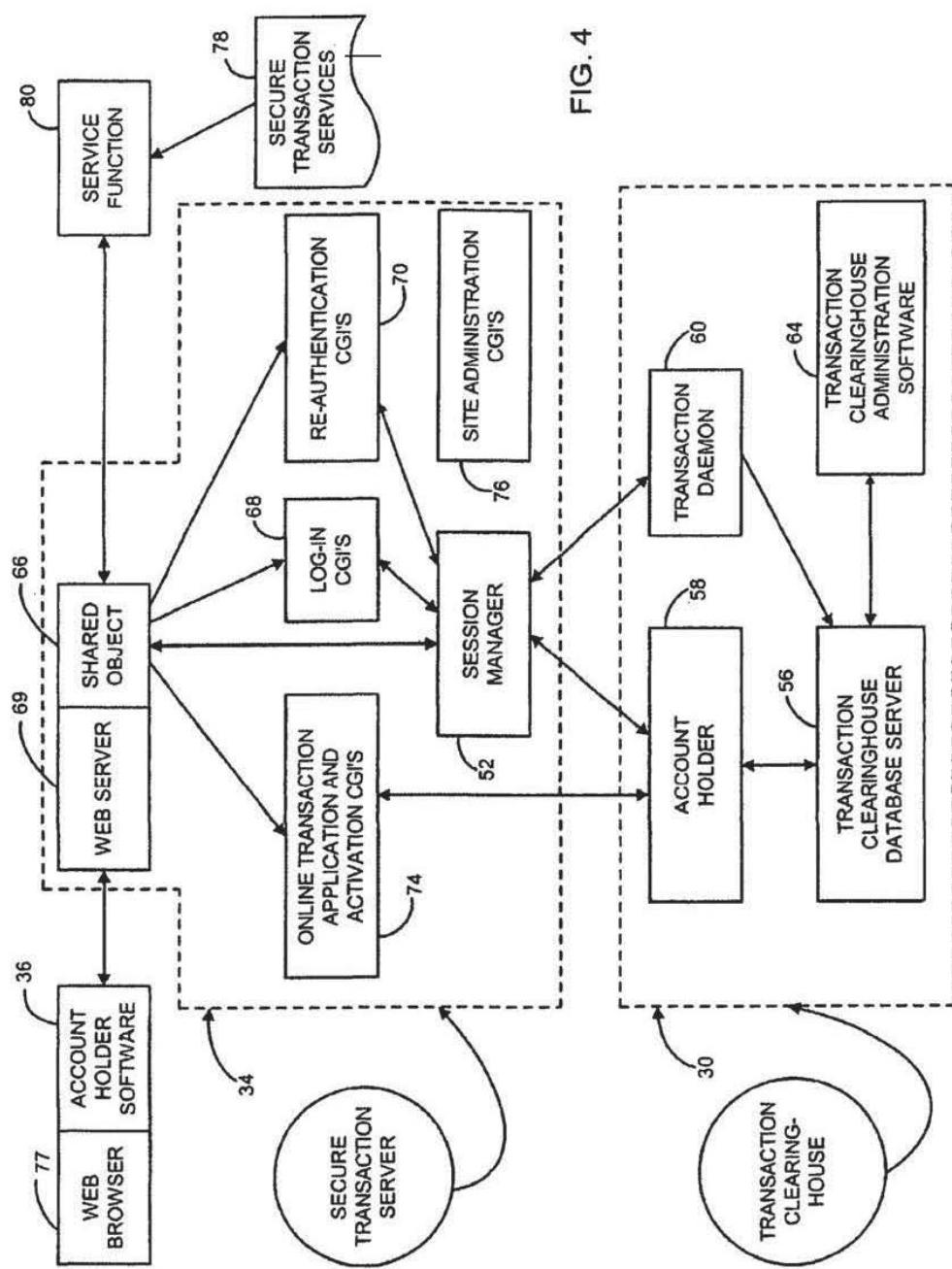


FIG. 3



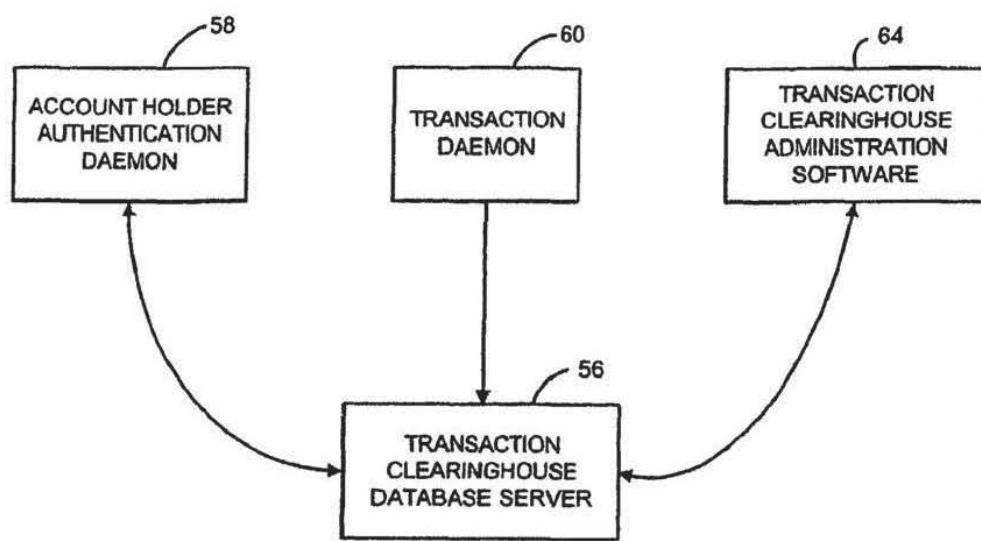


FIG. 5

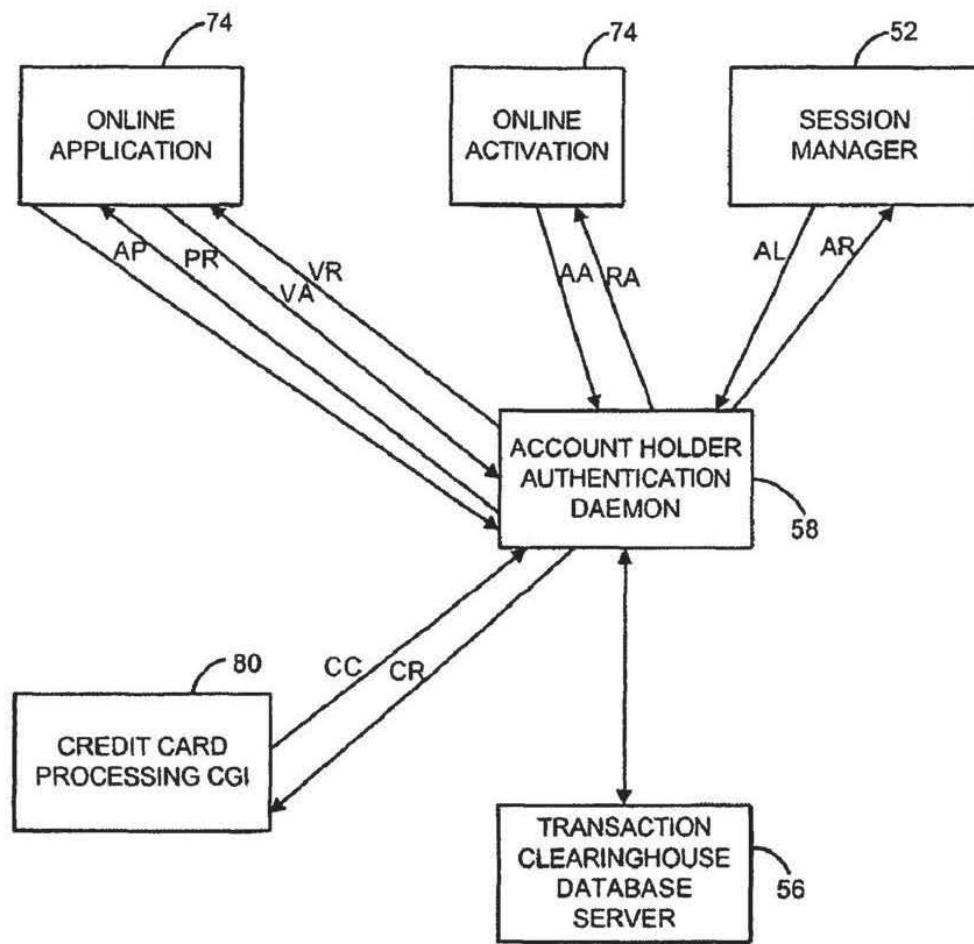


FIG. 6

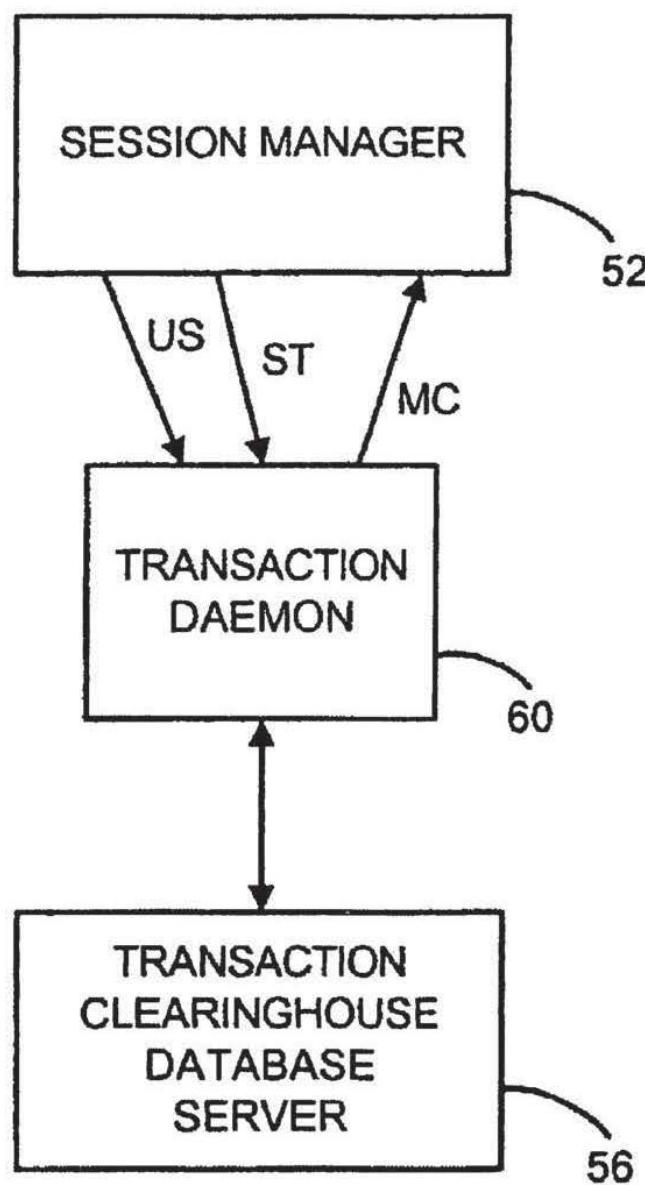


FIG. 7

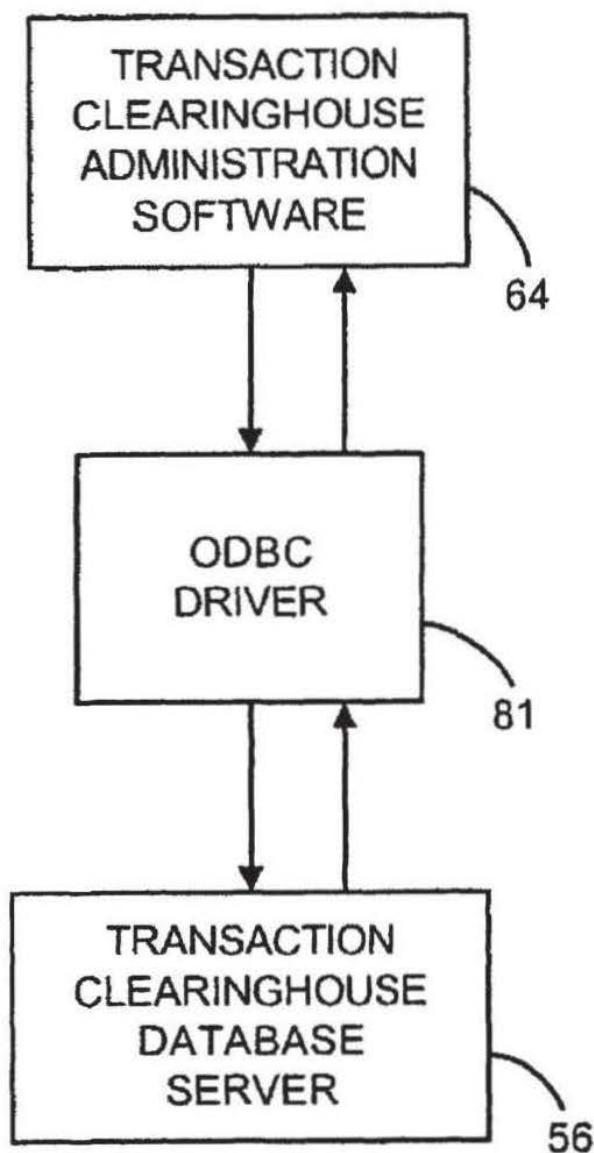


FIG. 8

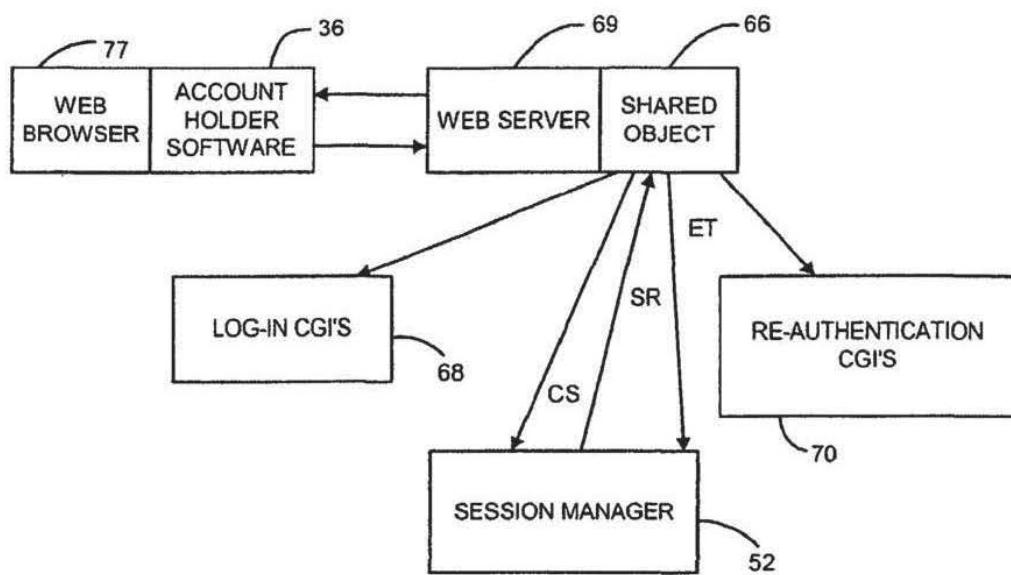


FIG. 9

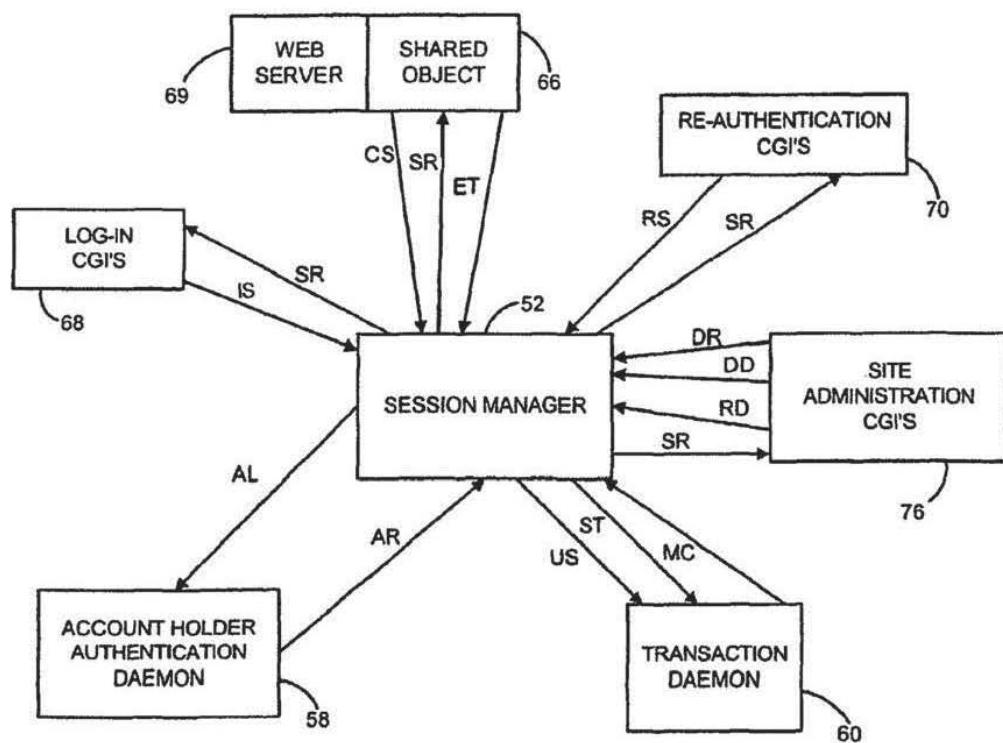


FIG. 10

TX0001-0030

Appx137

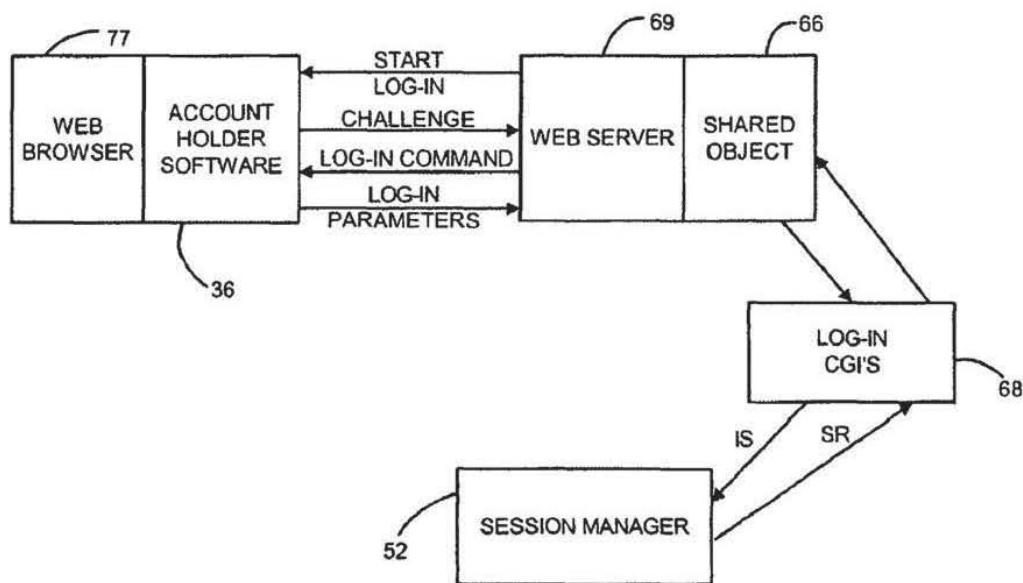


FIG. 11

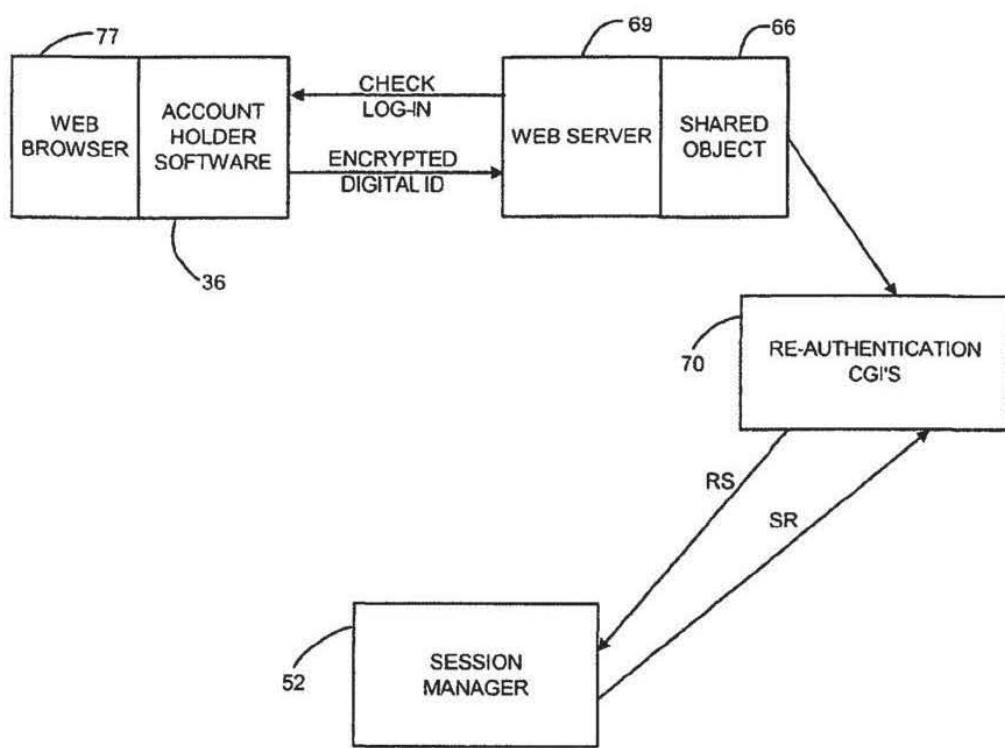


FIG. 12

TX0001-0032

Appx139

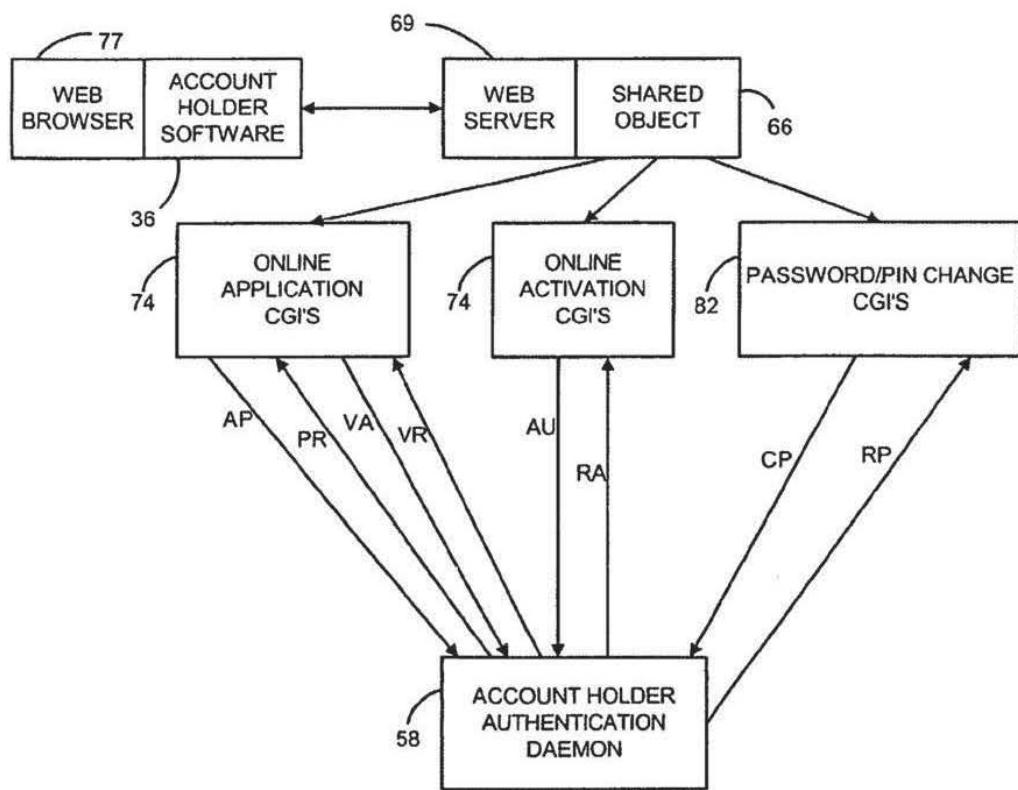


FIG. 13

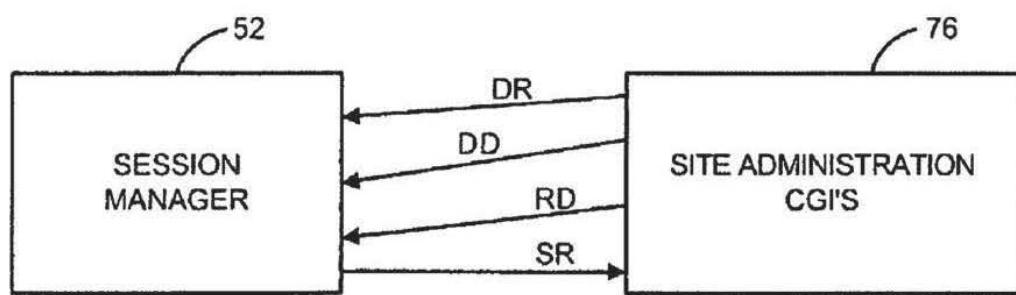
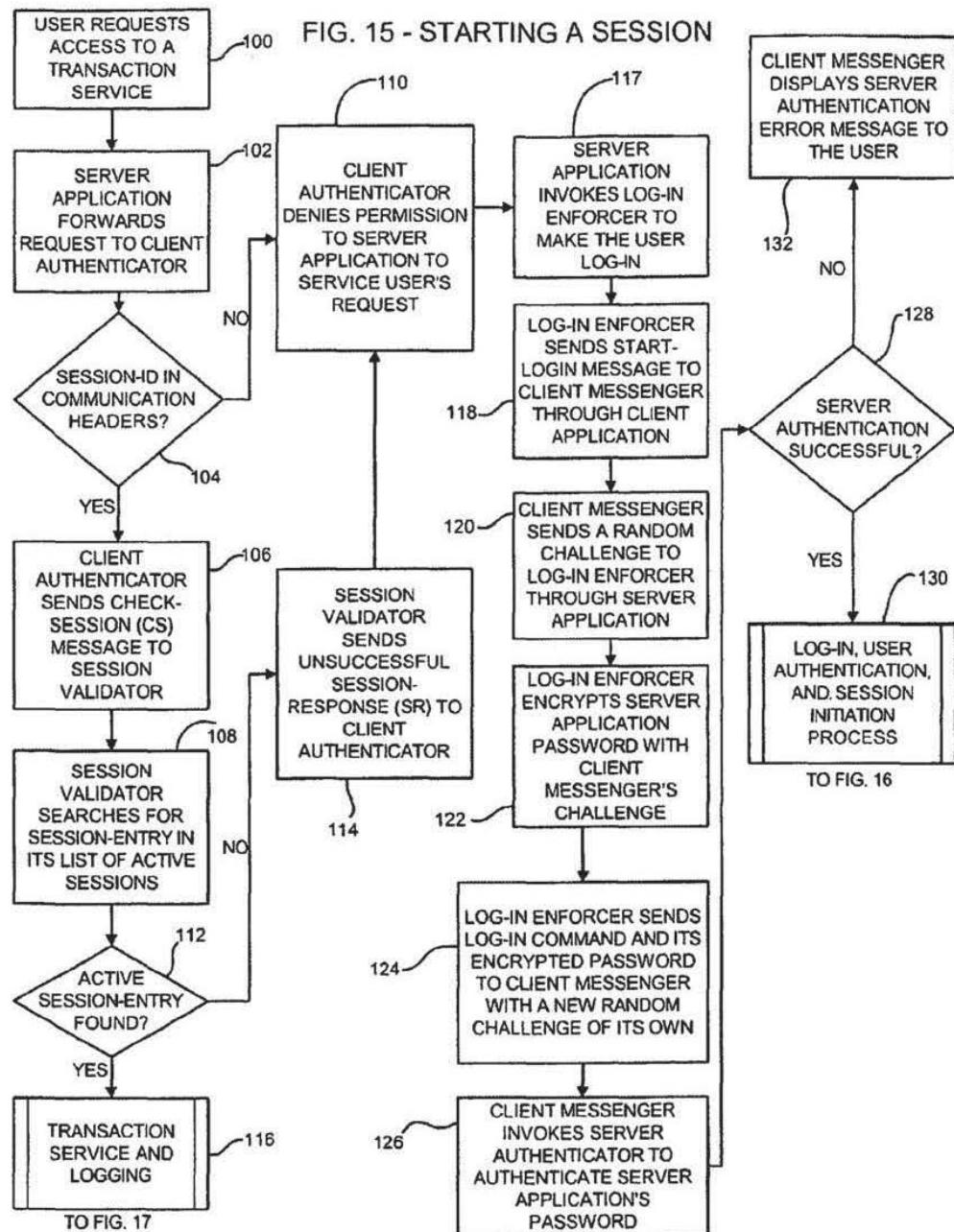


FIG. 14



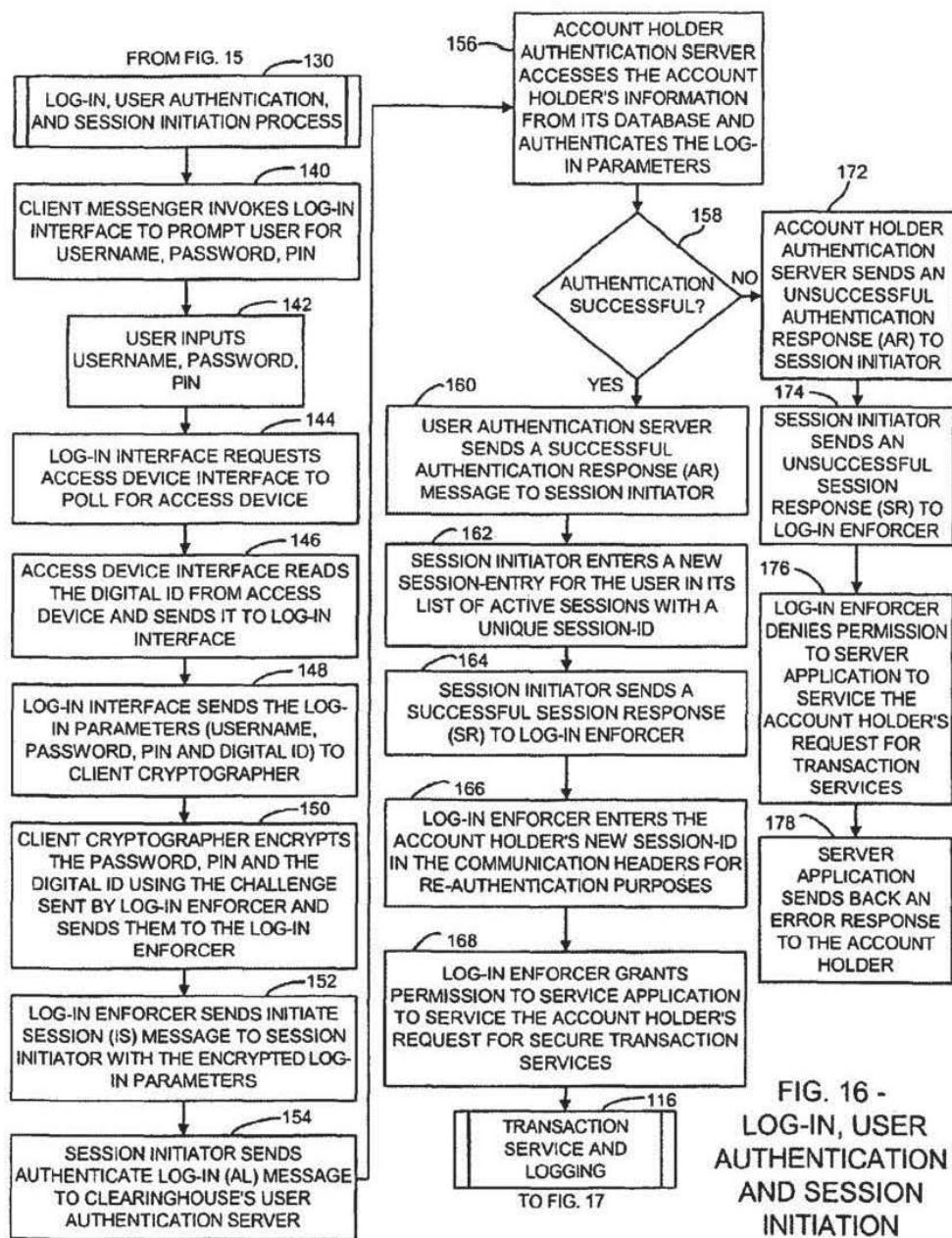


FIG. 16 -  
LOG-IN, USER  
AUTHENTICATION  
AND SESSION  
INITIATION

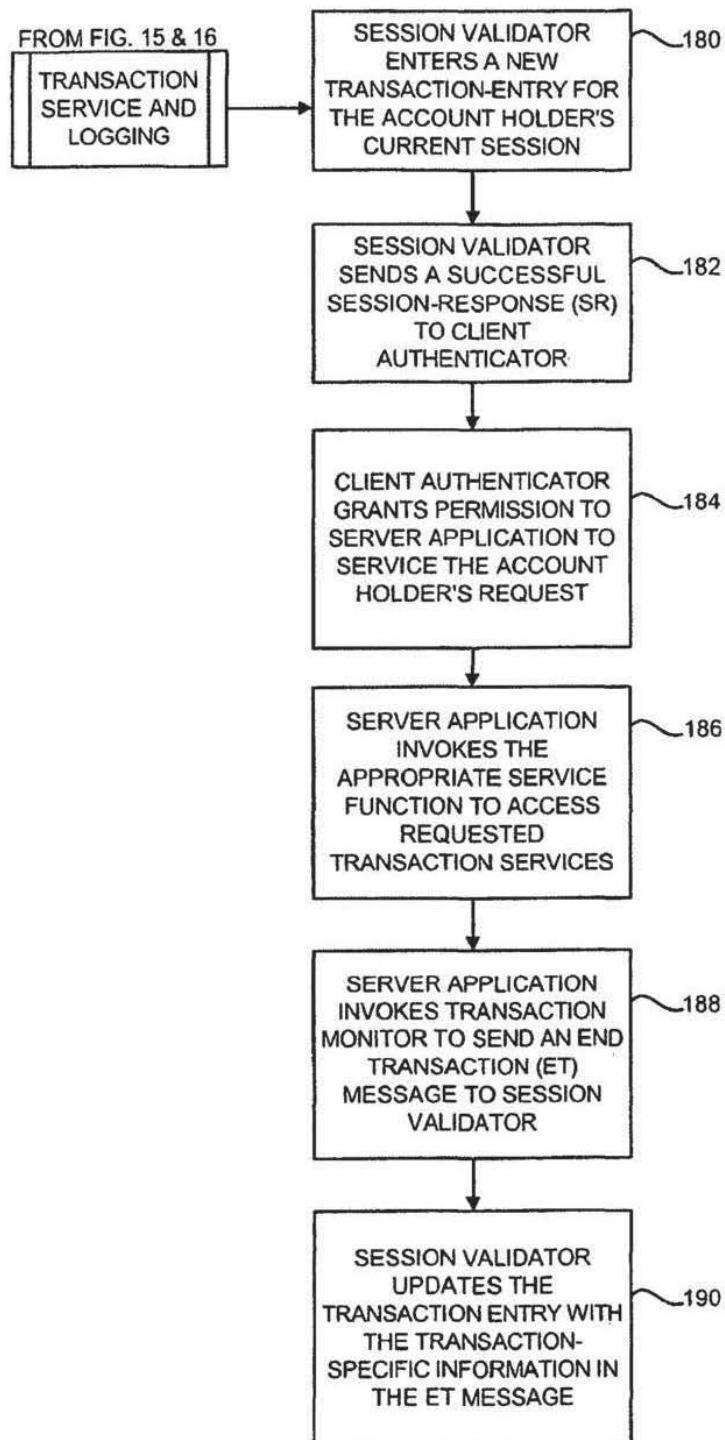
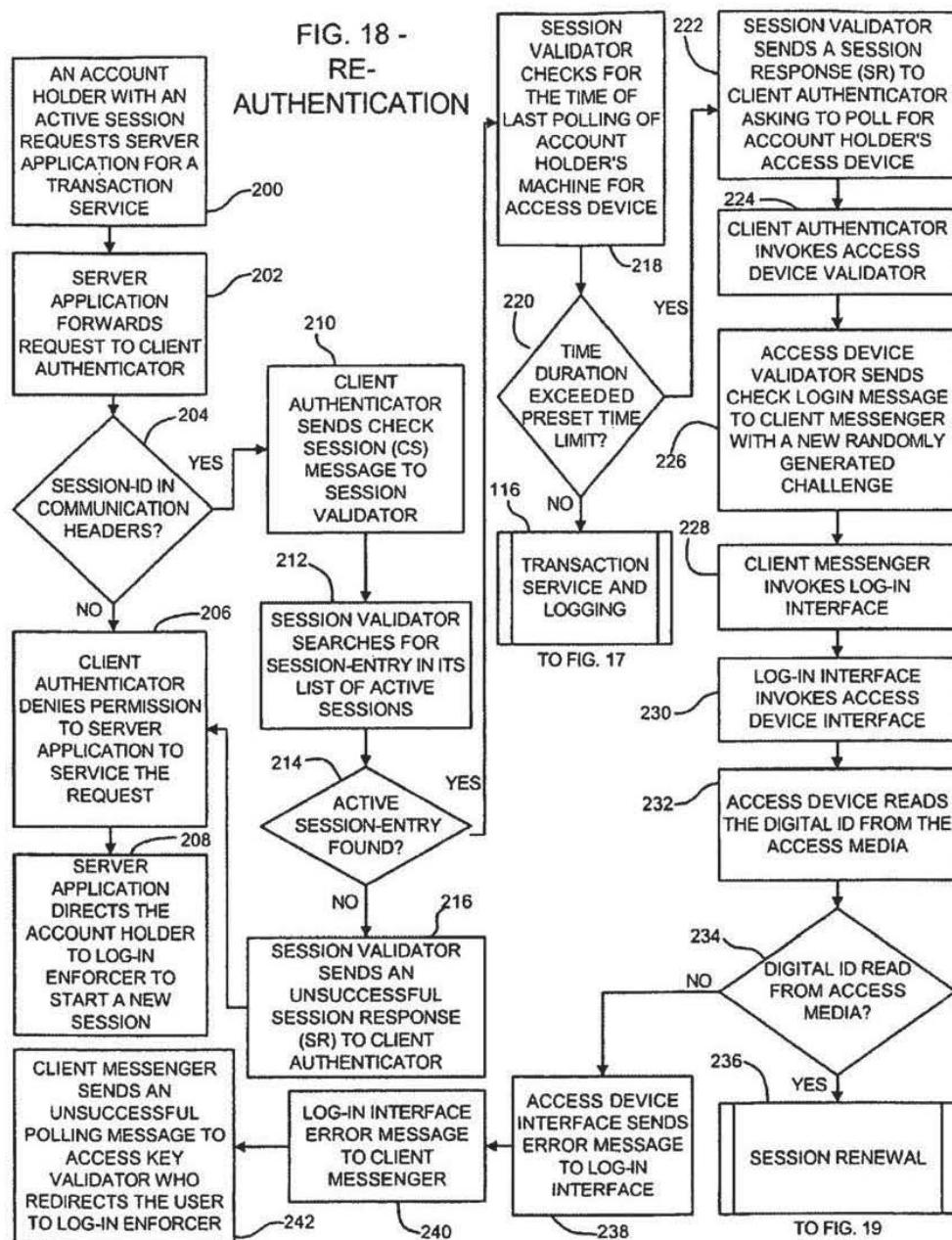
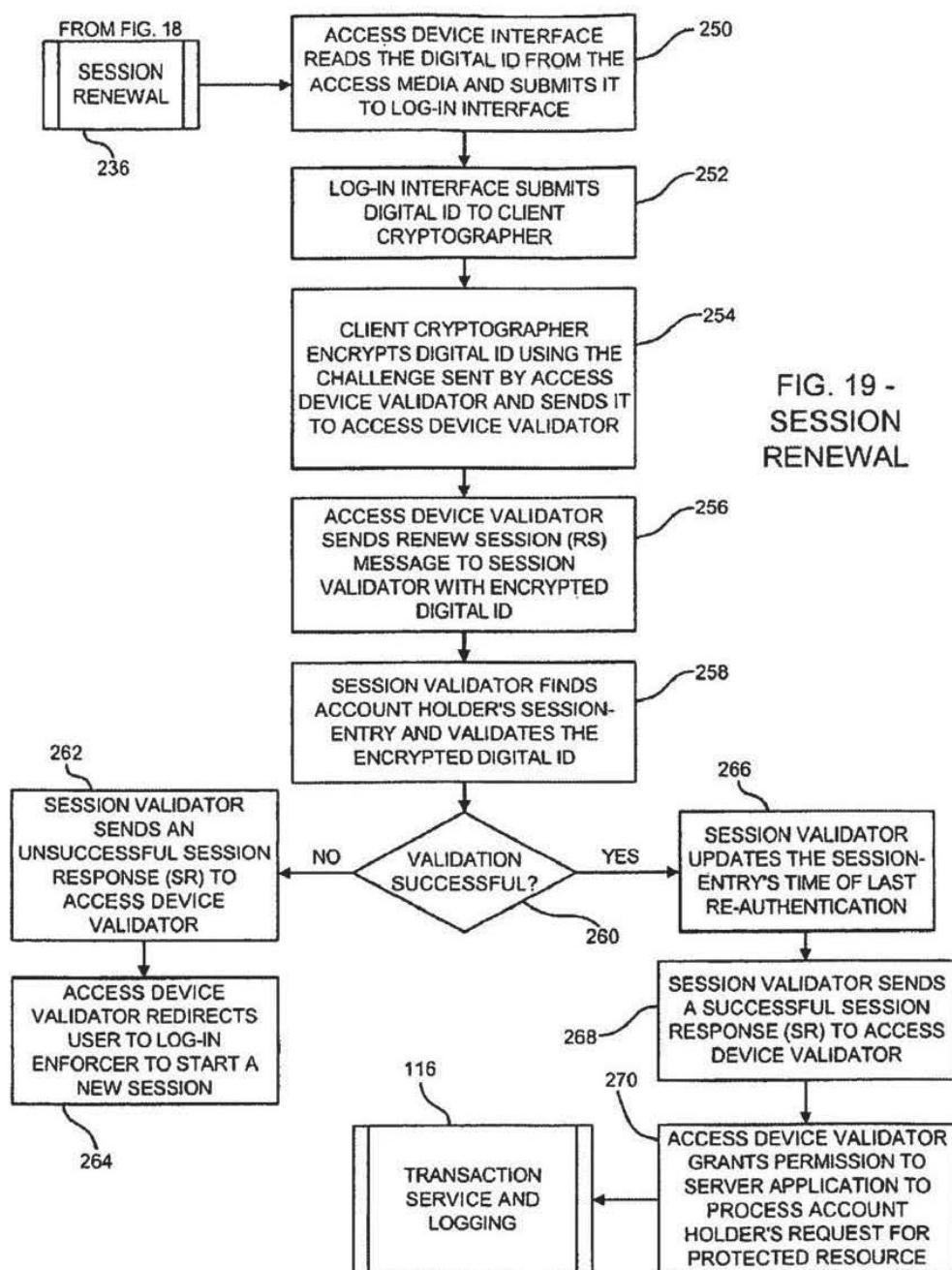
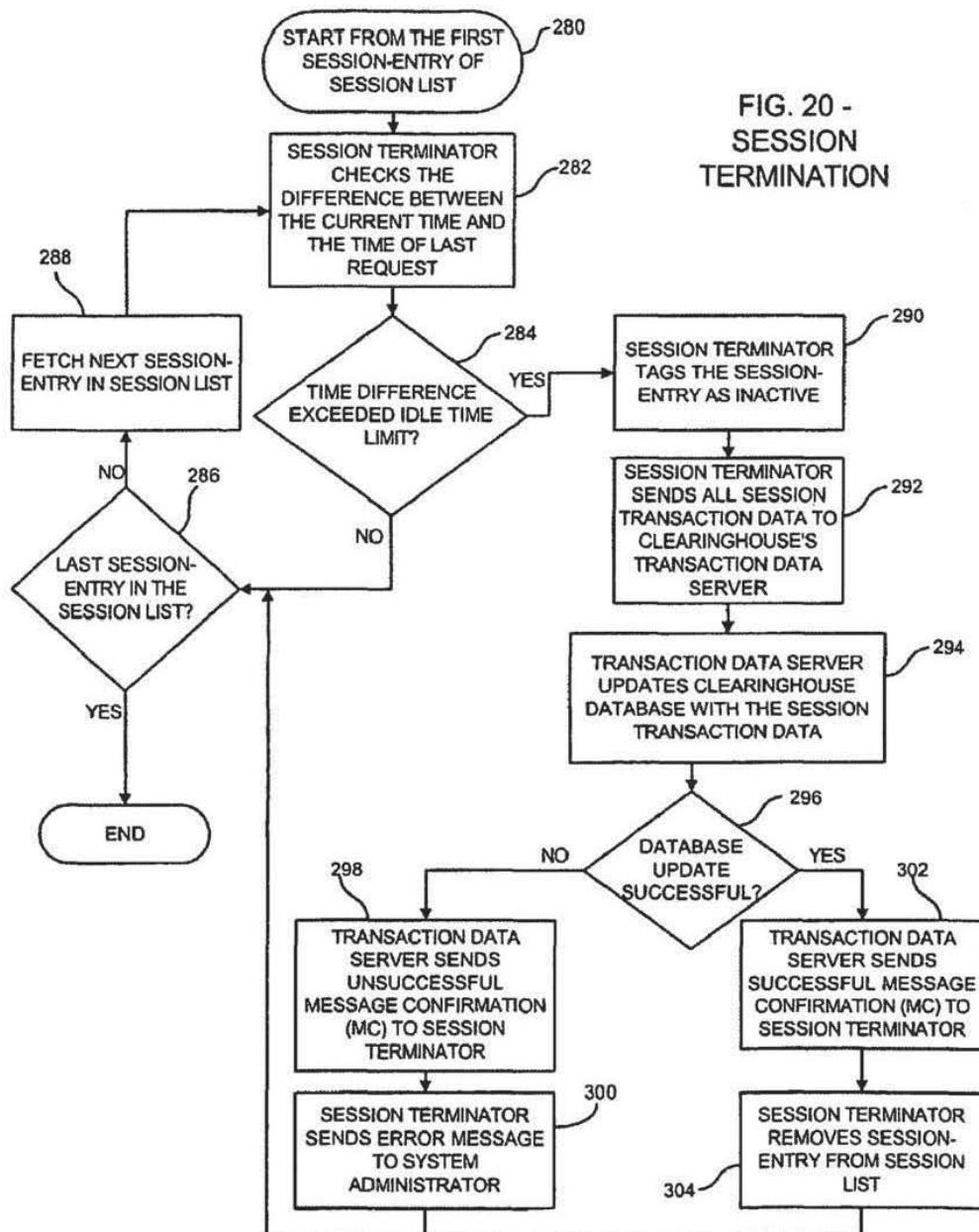


FIG. 17 - TRANSACTION SERVICE AND LOGGING







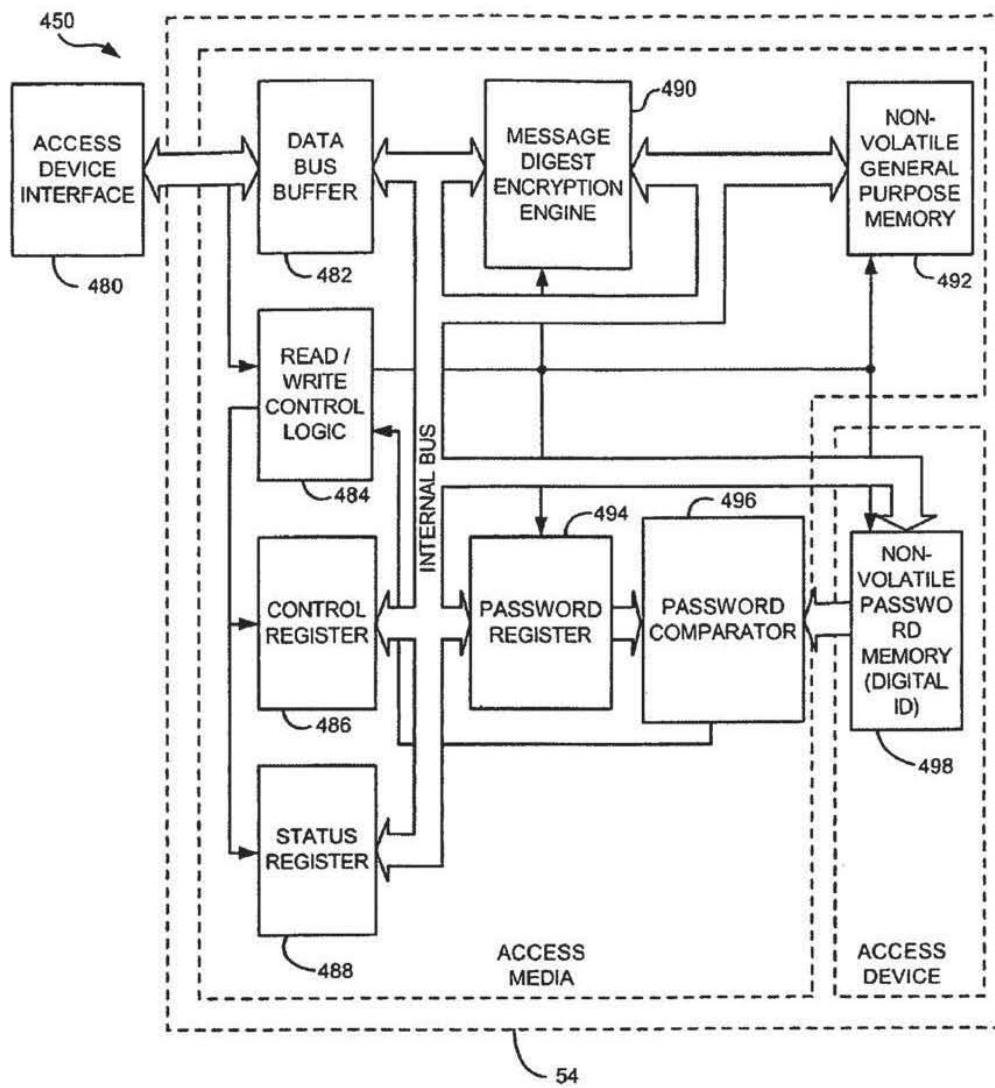


FIG. 21 -  
HARDWARE TOKEN  
ACCESS DEVICE

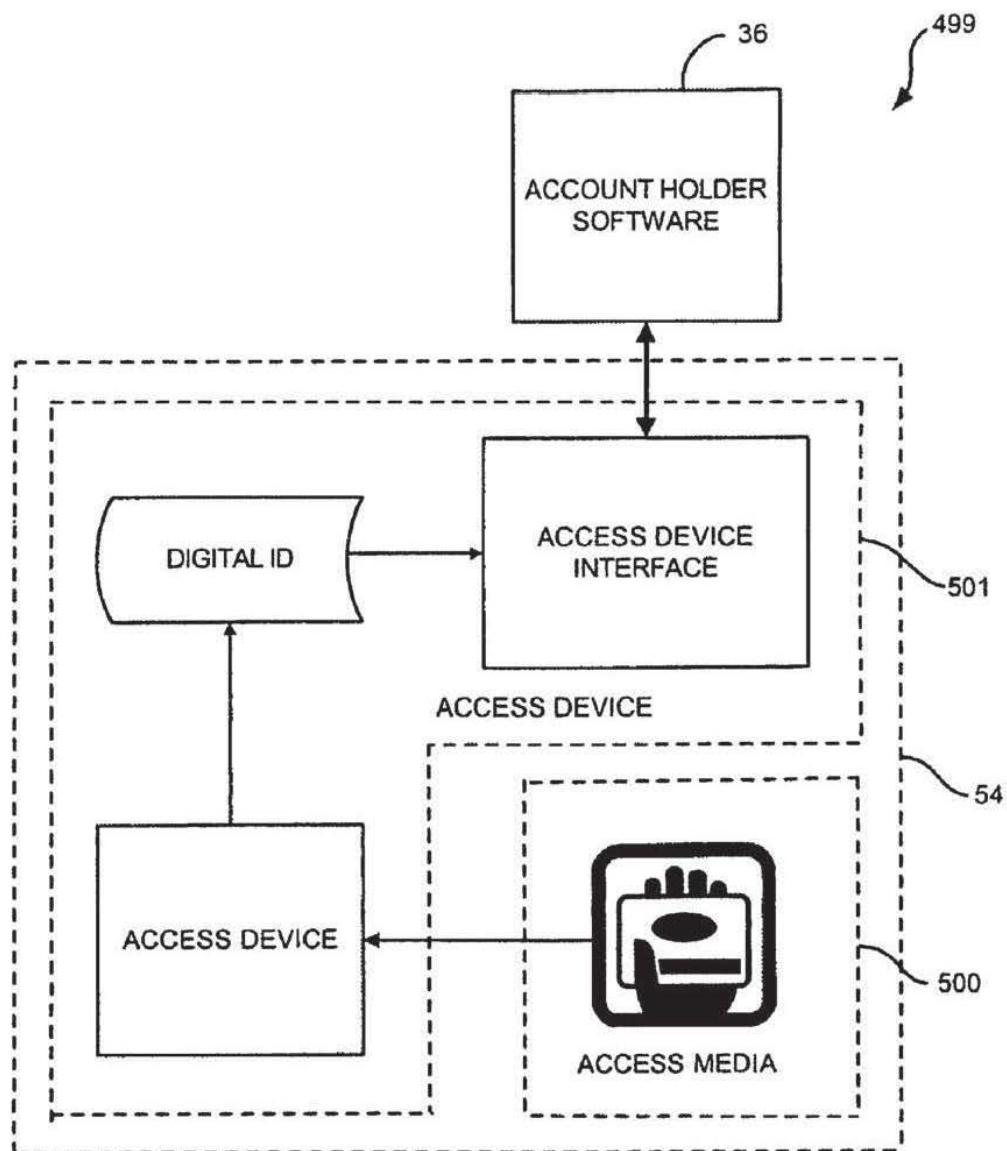


FIG. 22 -  
MAGNETIC CARD ACCESS DEVICE

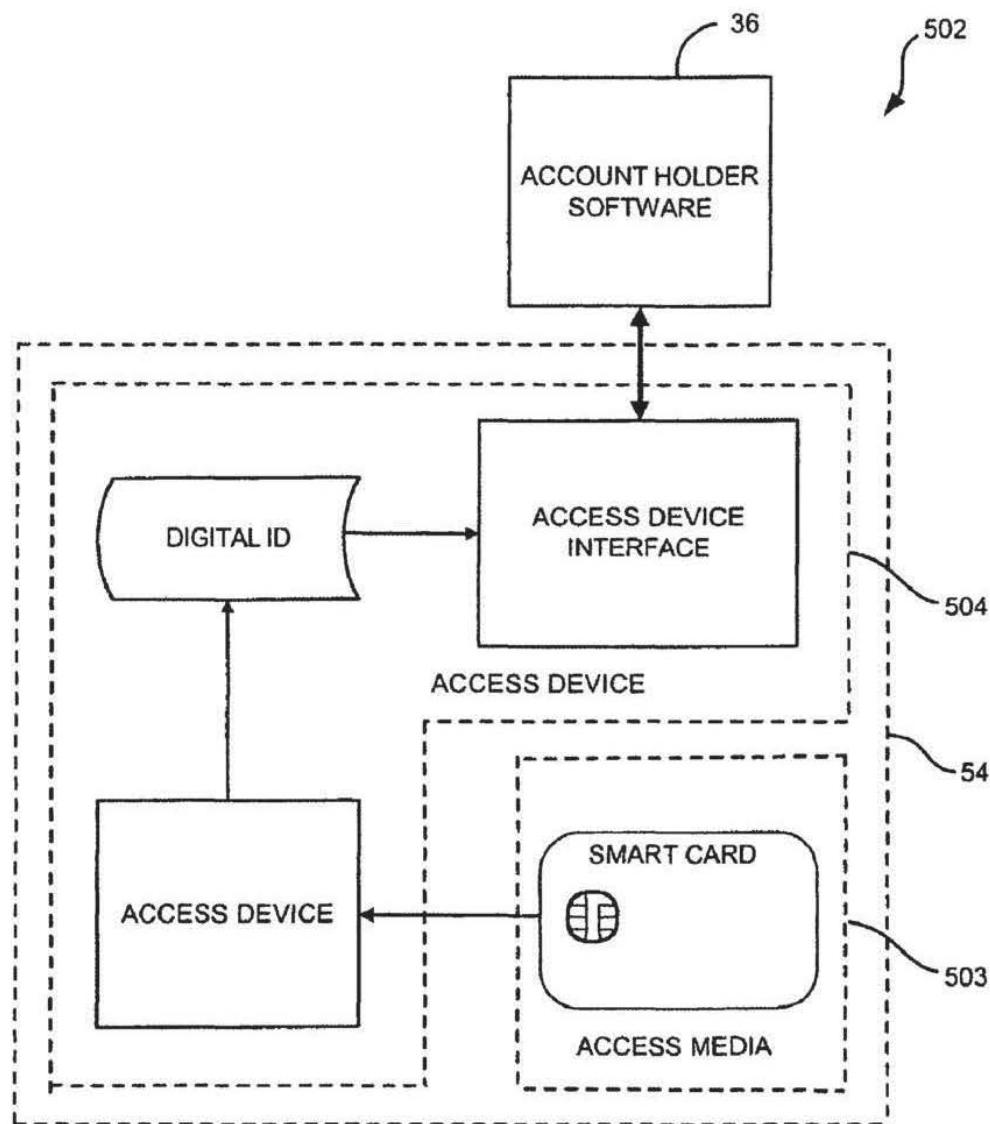


FIG. 23 -  
SMART CARD ACCESS DEVICE

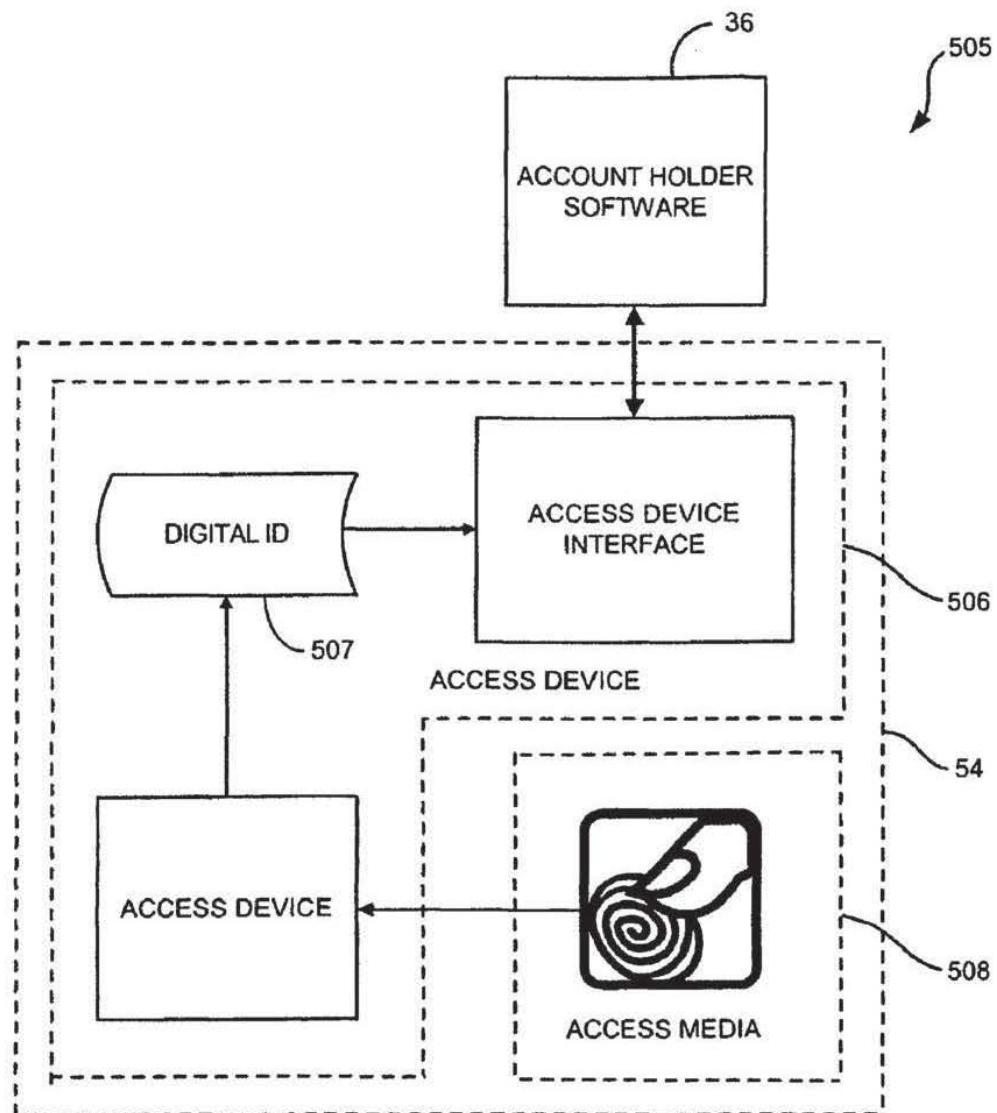


FIG. 24 -  
BIOMETRIC IDENTIFICATION ACCESS DEVICE

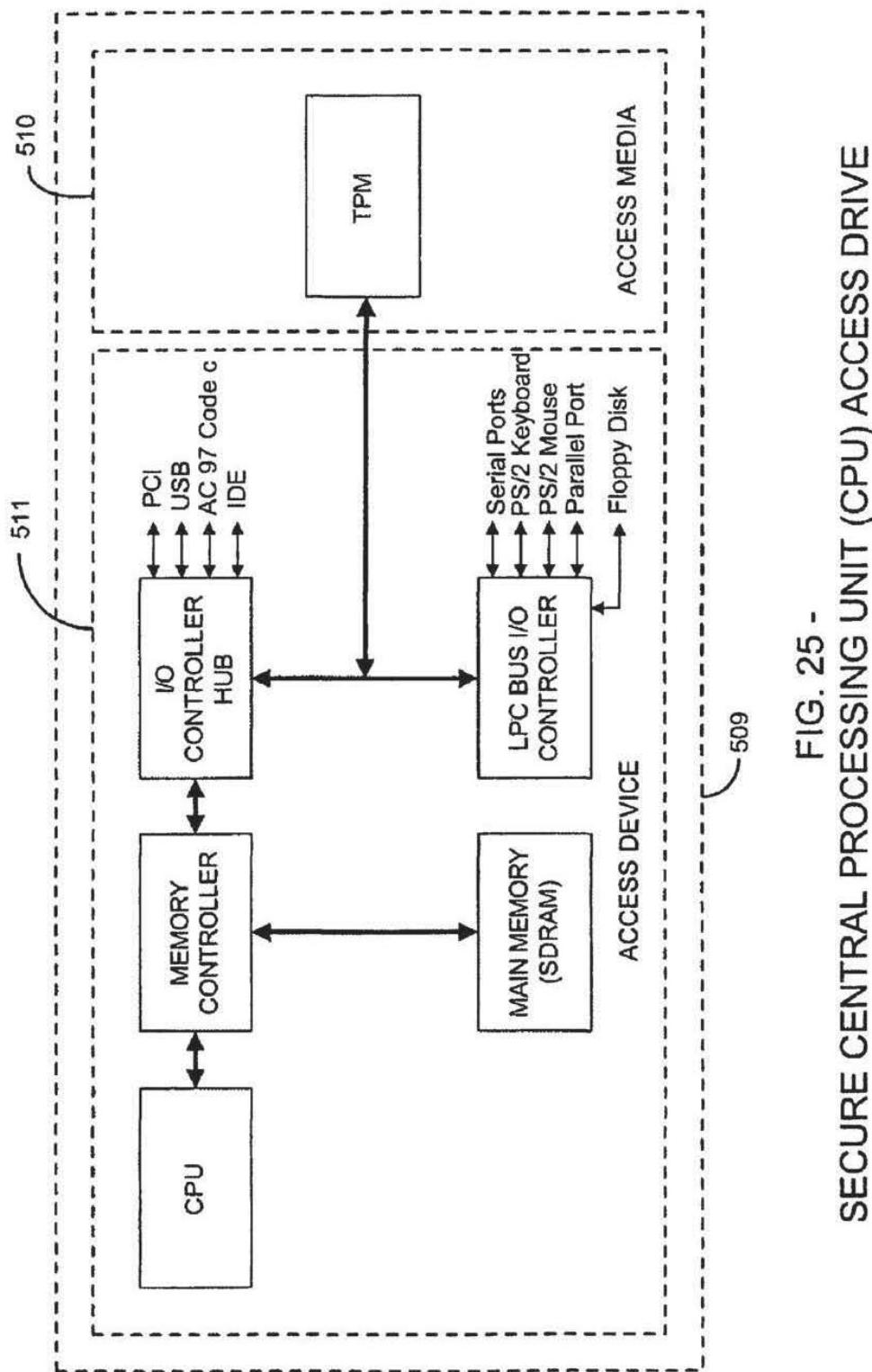


FIG. 25 -  
SECURE CENTRAL PROCESSING UNIT (CPU) ACCESS DRIVE

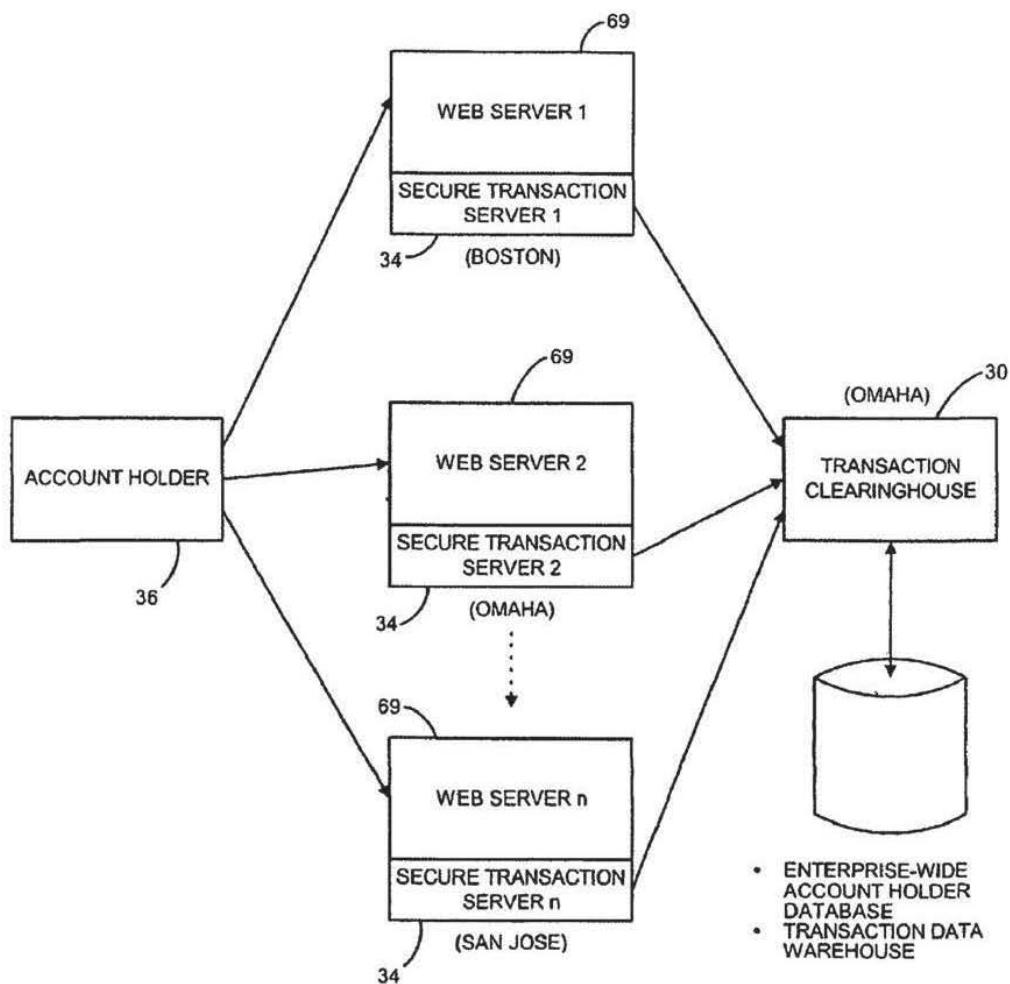


FIG. 26 -  
MULTIPLE SECURE TRANSACTION SERVERS WITH A  
SINGLE TRANSACTION CLEARINGHOUSE

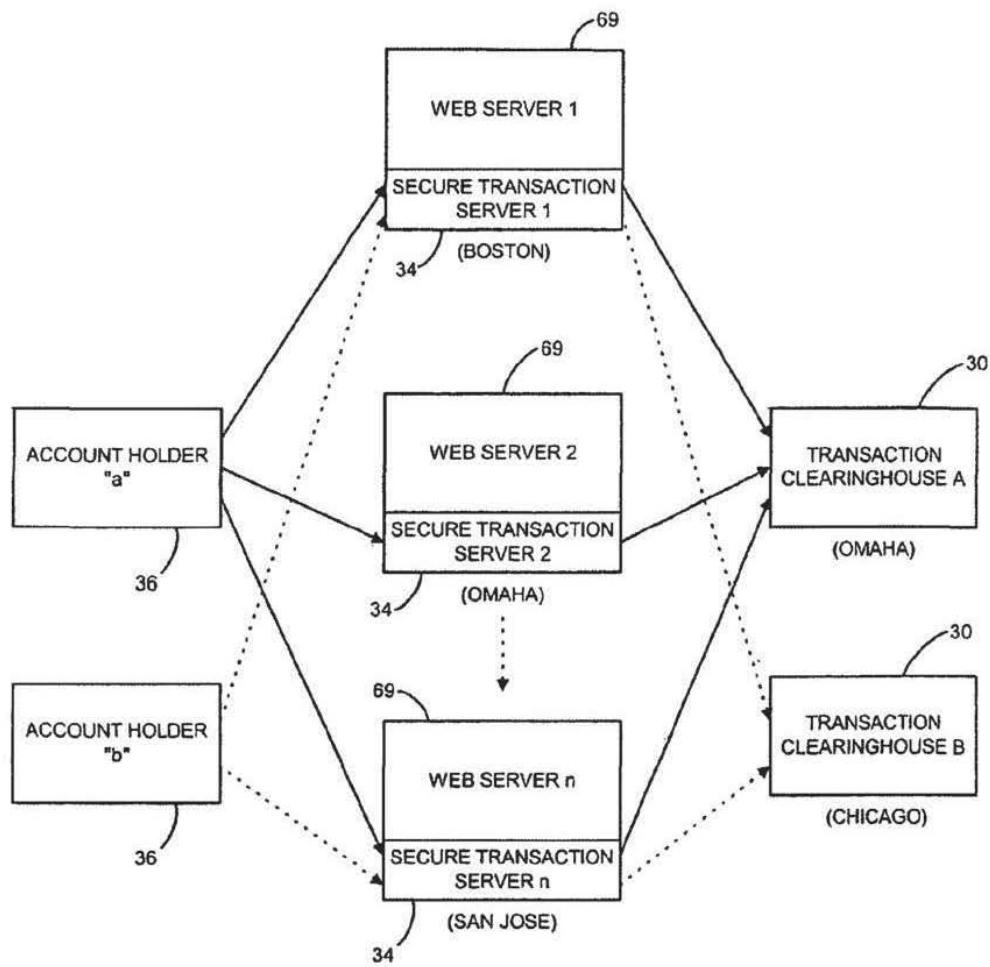


FIG. 27 -  
MULTIPLE SECURE TRANSACTION SERVERS WITH  
MULTIPLE TRANSACTION CLEARINGHOUSES

1

**METHOD AND SYSTEM FOR MANAGING  
ACCESS TO PROTECTED COMPUTER  
RESOURCES PROVIDED VIA AN INTERNET  
PROTOCOL NETWORK**

The present application is a continuation of application Ser. No. 10/230,638, filed Aug. 29, 2002, now U.S. Pat. No. 7,290,288; which is incorporated herein by reference; and which is a continuation-in-part of application Ser. No. 08/872,710, filed Jun. 11, 1997, now U.S. Pat. No. 6,516,416.

**BACKGROUND OF THE INVENTION**

1. Field of the Invention

The present invention generally relates to security systems for use with computer networks. More particularly, the present invention relates to a secure transaction system that is particularly adapted for use with untrusted networks, such as the Internet.

2. Description of the Prior Art

There are many businesses that are connected to the Internet or some other untrusted network. Such businesses may provide transaction services without charge for certain transactions that can be accessed by any account holder having access to the network. However, the same business may want to generate revenue from other transaction services and also to protect its business assets. In order to generate revenue, there must be control over account holder access, transaction tracking, account data, and billing. For a business to offer transaction services on an untrusted network, such as the web, it must have access to a web server that connects to the Internet. Any account holder with a web browser can then access the web site.

To implement a secure transaction system for use over the web, businesses need to implement authentication, authorization and transaction tracking. Authentication involves providing restricted access to transaction services that are made available, and this is typically implemented through traditional account holder name-password schemes. Such schemes are vulnerable to password fraud because account holders can share their usernames and password by word of mouth or through Internet news groups, which obviously is conducive to fraudulent access and loss of revenue. Authorization, on the other hand, enables authenticated account holders to access transaction services based on the permission level they are granted. Transaction tracking involves collecting information on how account holders are using a particular web site, which traditionally involved the data mining of web server logs. This information is often inadequate to link web site transaction and a particular account holder who used the web site. There is also no generic transaction model that defines a web transaction, which contributes to the difficulty in implementing an account holder model based upon transactions. Thus, there is a need for an improved secure transaction system and method for securing and tracking usage by a client computer.

**SUMMARY OF THE INVENTION**

The present invention discloses a system for securing and tracking usage of transaction services or computer resources by a client computer from a first server computer, which includes clearinghouse means for storing identity data of the first server computer and the client computer(s); server software means installed on the first server computer and client software means installed on the client computer(s) adapted to forward its identity data and identity data of the client com-

2

puter(s) to the clearinghouse means at the beginning of an operating session; and a hardware key connected to the client computer, the key being adapted to generate a digital identification as part of the identity data; the server software means being adapted to selectively request the client computer to forward the identification to the first server computer for confirmation of the hardware key being connected; the clearinghouse means being adapted to authenticate the identity of the client computer responsive to a request for selected services or resources of the first server computer; the clearinghouse means being adapted to authenticate the identity of the first server computer responsive to the client computer making the request; and the clearinghouse means being adapted to permit access to the selected request responsive to successful initial authentication of the first server computer and the client computer making the request; wherein the hardware key is implemented using a hardware token access system, a magnetic card access system, a smart card access system, a biometric identification access system or a central processing unit with a unique embedded digital identification.

These and other objects of the present invention will be apparent from review of the following specification and the accompanying drawings.

**BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 is a block diagram of the secure transaction system embodying the present invention, wherein a secure transaction server is part of a local area network, with the server being connected to the Internet and to the local area network via a firewall;

FIG. 2 is a functional block diagram of the secure transaction system embodying the present invention and illustrating the functional interaction of components of the system and a account holder;

FIG. 3 is a more detailed block diagram of the schema of the present invention;

FIG. 4 is a software block diagram illustrating the system architecture of the preferred embodiment in the web environment, also known as the secure transaction system;

FIG. 5 is a functional block diagram illustrating the structure and operation of the transaction clearinghouse database server process of the preferred embodiment;

FIG. 6 is a functional block illustrating the structure and operation of the transaction clearinghouse account holder authentication daemon of the preferred embodiment;

FIG. 7 is a block diagram illustrating the structure and operation of the transaction daemon of the preferred embodiment;

FIG. 8 is a functional block diagram illustrating the structure and operation of the transaction clearinghouse administration software of the preferred embodiment;

FIG. 9 is a functional block diagram illustrating the structure and operation of the server shared object of the preferred embodiment;

FIG. 10 is a functional block diagram illustrating the structure and operation of the server session manager of the preferred embodiment;

FIG. 11 is a functional block diagram illustrating the structure and operation of the server login common gateway interface (CGI) program of the preferred embodiment;

FIG. 12 is a functional block diagram illustrating the structure and operation of the server re-authentication common gateway interface (CGI) program of the preferred embodiment;

FIG. 13 is a functional block diagram illustrating the structure and operation of the server online application and activation common gateway interface (CGI) program of the preferred embodiment;

FIG. 14 is a functional block diagram illustrating the structure and operation of the server site administration common gateway interface program of the preferred embodiment;

FIG. 15 is a flow chart of the operation of the system at the start of a session where a account holder requests access to a secure transaction;

FIG. 16 is a flow chart of the system illustrating the steps that are taken during the login, account holder authentication and session initiation;

FIG. 17 is a flow chart of the sequence of steps that occur during transaction service and login;

FIG. 18 is a flow chart of the sequence of steps taken during a re-authentication operation;

FIG. 19 is a flow chart of the sequence of steps that occur during a session renewal;

FIG. 20 is a flow chart of the sequence of steps that occur during a session termination;

FIG. 21 is a block diagram of the hardware token access device that is part of the preferred embodiment of the present invention;

FIG. 22 is a block diagram of the magnetic card reader access device and access media that is part of the preferred embodiment of the present invention;

FIG. 23 is a block diagram of the smart card reader access device and access media that is part of the preferred embodiment of the present invention;

FIG. 24 is a block diagram of the biometric identification reader access device and access media that is part of the preferred embodiment of the present invention;

FIG. 25 is a block diagram of the secure central processing unit (CPU) access device and access media that is part of the preferred embodiment of the present invention;

FIG. 26 is a functional block diagram which illustrates multiple system servers with a single system transaction clearinghouse; and

FIG. 27 is a functional block diagram illustrating a system having multiple system servers and multiple system transaction clearinghouses.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Broadly stated, the present invention is directed to a secure transaction system that is particularly adapted for use with an untrusted network, such as the Internet worldwide web. As used herein, an untrusted network is defined as a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous. A client-server application running over such a network has no control over the transmitted information during all the phases of transmission. The present invention provides a platform for securing transactions between consumers and suppliers on an untrusted network. Because of its superior design and operation, it is capable of operating servers and transaction clearinghouses in a geographically distributed fashion. The present invention implements its platform by restricting transaction services to only authenticated and authorized account holders and by tracking their transaction in a generic transaction model that can be easily integrated to any billing model.

The system has four major components as shown in FIG. 1, which are a transaction clearinghouse, indicated generally at 30; account holder administration software, shown generally

at 32; a secure transaction server, indicated generally at 34; and a number of account holder software, one of which is shown generally at 36. The account holders are connected to the Internet 38 via a modem connection or a similar means, and the Internet 38 has a connection to the server. The server 34 is connected to a local area network (LAN) 40 through a firewall computer 42. A firewall is used to separate a local area network from the outside world. In general, a local area network is connected to the outside world by a "gateway" computer. This gateway machine can be converted into a firewall by installing special software that does not let unauthorized TCP/IP packets passed from inside to outside and vice versa. The LAN 40 also provides a connection to the account holder administration software 32 and to the transaction clearinghouse 30. While the configuration shown in FIG. 1 has a single secure transaction server 34 and a single transaction clearinghouse server 30, the secure transaction system of the present invention is adapted to be used in other configurations, which may include multiple secure transaction servers being controlled by a single transaction clearinghouse 30 or multiple secure transaction servers that interact with multiple transaction clearinghouses 30. Such flexibility in configurations is an extremely desirable aspect of the present invention.

With respect to the major components of the system as shown in FIG. 1, the transaction clearinghouse 30 preferably resides on a back office platform in a corporate network. It has a secure interface to communicate with the secure transaction servers 34, which reside on the same machine that hosts the web server. The account holder software, on the other hand, resides on the account holder's desktop machine. The transaction clearinghouse server is preferably a Sun UNIX server which runs the transaction clearinghouse server processes and the database server. However, the database server could reside on a separate machine. The transaction clearinghouse is the entity that hosts all of the account and transaction data. The transaction clearinghouse provides a secure interface to the secure transaction servers 34, which enables the secure transaction servers 34 to authenticate the account holders and to send account holders' transaction data to the transaction clearinghouse. The transaction clearinghouse consists of a structured query language (SQL) database, which hosts the transaction clearinghouse database as well as an account holder authentication server for authenticating account holders on behalf of the secure transaction servers and processes online applications. The transaction clearinghouse also includes a transaction server that collects transaction data from the secure transaction servers 34 and updates the transaction clearinghouse database. The transaction clearinghouse also includes administration software 32 that provides a thin client graphical user interface to administer the transaction clearinghouse database.

With respect to the transaction clearinghouse administration software 32, it preferably resides on a desktop PC with a browser and is connected to the LAN 40 so that it can communicate with the transaction clearinghouse database server 30. This software will typically be on the LAN 40 of the organization so that database access through the administration software 32 is restricted within the organization. Using this administration software, an administrator can define the configuration for the account holder services, administer accounts, demographic data and transaction data. In the present invention, it is contemplated that the demographic data can be personal profile information, which may include at least two of the following items of information including: e-mail address, username, password, personal identification number, billing name, billing address, billing city, billing

state, billing zip code, billing country, shipping name, shipping address, shipping city, shipping state, shipping zip code, shipping country, shipping method, home phone number, work phone number, cellular phone number, facsimile phone number, credit card number, credit card expiration date, credit card type, debit card number, debit card expiration date, debit card type, card-holders name, date of birth, and social security number.

With respect to the secure transaction server 34, the software for it is preferably located on the same machine that hosts the web server. It is preferably a Sun Solaris machine or comparable computer. The secure transaction server 34 operates in conjunction with the transaction clearinghouse to authenticate and authorize account holders and to collect their transaction data. The secure transaction server 34 also interacts with the account holder software at the account holder computer 36 to provide transaction capture. The secure transaction server 34 consists of a shared object that is incorporated as a part of the web server software. It also has a collection of common gateway interface programs (CGI's) that implement authentication tasks, such as login and access device polling. A session manager is provided for building sessions for every valid account holder so that a transaction list that contains all of the tasks performed during a account holder's session can be kept. The server also includes a thin client site administration software program that provides a web based visual interface to administer the session manager and maintain account holder profiles. The server sends transaction data to the transaction clearinghouse at the end of every account holder's session and includes added functionality for processing and activating online account applications.

The account holder computer 36 includes software that enables an account holder's web browser to access the untrusted network. The account holder desktop PC contains a browser to access the untrusted network and also includes account holder software for enabling the account holder to access secure transaction services. The account holder software, in addition to enabling the access to a web site providing secure transaction services, also allows for enforcement of the login process, re-authentication process and transaction tracking. All of these features are controlled by the secure transaction server 34, which sends specific commands to the account holder software 36 to perform the tasks as needed. The account holder software is a plug-in or control that adds secure transaction functionality to standard browser software. The account holder also includes a hardware key for providing two or three factor authentication. FIGS. 21-25 illustrate the hardware key, which include a hardware token, magnetic card reader, smart card reader, or biometric identification reader connected to each account holder's client computer or alternatively a secure central processing unit as part of the account holder's client computer capable of reading access media that generates a unique digital ID.

The account holder access components preferably use the transmission control protocol/internet protocol (TCP/IP) and transaction datagram protocol/internet protocol (UDP/IP) to communicate with each other. Any communication that needs to go through the web server or the web browser will follow the hyper text transfer protocol (HTTP) which is based on TCP/IP. These protocols are well known to those skilled in the art. The account holder's PC accesses web sites using HTTP. The web server and secure transaction server 34 communicate with each other using UDP/IP. The secure transaction server 34 and the transaction clearinghouse 30 preferably communicate with each other using TCP/IP and the transaction clearinghouse servers communicate with a database using open database connectivity (ODBC) drivers most com-

monly over a TCP/IP network. The transaction clearinghouse administration software 32 communicates with the database using an ODBC driver, most commonly over a TCP/IP or IPX network.

5 The four main components of the preferred embodiment of the system as described with respect to FIG. 1 interact with one another using a distributed architecture which establishes a many-to-many relationship between the secure transaction servers 34 and the transaction clearinghouse 30. One transaction clearinghouse 30 can be monitoring multiple secure transaction servers 34 while each secure transaction server is interacting with multiple account holders 36. Similarly, a secure transaction server 34 can be configured to interact with multiple transaction clearinghouses 30.

10 The manner in which the preferred embodiment of the system operates in the web environment can be broadly seen by the functional block diagram of FIG. 2, which shows the transaction clearinghouse server 30, secure transaction server 34, and account holder 36 with steps that are taken during a session. The first step is for the account holder software 36 to request transaction services and that request is communicated to the secure transaction server 34 that then commands the account holder to login. The account holder software 36 inputs the login parameters that the secure transaction server 34 then forwards to the transaction clearinghouse. If the parameters are valid, the transaction clearinghouse 30 provides a response to the secure transaction server 34 that then enables the account holder software 36 to access the transaction services. The session transaction data is eventually forwarded for storage by the transaction clearinghouse 30.

15 While the steps that have been described with respect to FIG. 2 are a very broad overview of the preferred embodiment, the functional block diagram of FIG. 3 provides a more detailed general schema of the present invention. The system includes a server application 44, an account holder or client application 46, both of which are connected to an untrusted network via a traditional communication path indicated by the dotted lines 48 and 50. The system includes a session manager 52 for interacting with the transaction clearinghouse 30 and the secure transaction server 34 and a hardware key 54 which is connected to the account holder software 36. The solid lines connecting the blocks of the numbered components of FIG. 3 represent secure communications whereas the dotted lines are conventional communication paths that may not be secure.

20 Rather than describe the functions of the blocks of FIG. 3, the manner in which these components function will be described in connection with FIGS. 17-23, which provide more detailed flowcharts that relate to specific operations of the system.

25 The manner in which the system translates into the preferred embodiment in the web environment will be described in connection with the functional block diagram illustrated in FIG. 4. The transaction clearinghouse 30 contains the account and transaction database storage capability. The transaction clearinghouse 30 controls the authentication and authorization of account holders for individually enabled secure transaction web servers. The transaction clearinghouse 30 includes a number of subcomponents, including a transaction clearinghouse database server 56 that provides an open database connectivity (ODBC) interface to a structured query language (SQL) database that contains the account holder database and transaction data warehouse.

30 The transaction clearinghouse 30 also has an account holder authentication daemon 58 that processes the requests for account holder authentication by the secure transaction servers 34. A daemon 58 is a program that is not invoked

explicitly, but lays dormant waiting for one or more necessary conditions to occur such as an incoming request from one of its client programs. For every account holder authentication request, the account holder authentication daemon **58** first insures it is communicating with an authentic secure transaction server **34**, and then it queries the transaction clearinghouse database server **56** to find the account holder's information. Based on this information, it sends an authentication response back to the secure transaction server **34**. The account holder authentication daemon **58** also processes the secure transaction server's request for an online account holder application and an online account holder activation.

The transaction clearinghouse **30** also includes a transaction daemon **60** that is an independent server process that processes transaction data update requests made by secure transaction servers **34**. Similar to the account holder authentication daemon **58**, the transaction daemon **60** authenticates secure transaction servers before processing their requests. Upon successful authentication, it will accept all of the transaction data sent by a server and update the transaction clearinghouse database **56** with it. The transaction daemon **60** also authenticates secure transaction servers **34** before processing their request. The transaction clearinghouse **30** has administration software **64** that provides a visual interface on a computer with a web browser to administer the transaction clearinghouse database **56**.

With respect to the secure transaction server **34**, it runs in conjunction with a web server and is able to provide secure transaction services using the system of the present invention. The secure transaction server **34** authorizes each web transaction that involves account holder access of transaction services and does so by communicating with the account holder software **36** to make the account holders login. If the login is successful, the secure transaction server **34** initiates a session and collects all transaction data so that at the end of a session it can send the transaction data to the transaction clearinghouse. The secure transaction server also provides the functionality of session re-authentication. The secure transaction server includes a number of subcomponents including the session manager **52** which is a server process that processes messages sent by an account holder access shared object **66**, an account holder access common gateway interface programs (CGI's) **68** and the transaction clearinghouse **30**.

When an account holder **36** tries to log into a secure transaction system enabled web site, the session manager **52** communicates with the transaction clearinghouse **30** to authenticate the account holder. If successful, the session manager will start a new session for the account holder and from that point on, the account holder can access transaction services. Each web transaction during the session is reported to the session manager by the shared object **66** so that the session manager **52** can build a list of transactions for the account holder. At the end of the session, the session manager will send all of the session data and transaction data to the transaction clearinghouse **30** to update the database. If the system is utilizing two or three factor authentication (e.g., the user-name, password, PIN plus the digital ID generated by the access media read by the hardware key attached to the account holder's computer), the session manager **52** periodically communicates with the shared object **66** to perform re-authentication which involves polling of the account holder software **36** to insure that the hardware key **54** continues to be attached to the account holder computer.

The server shared object **66** is a binary module which provides function pointers to a web server **69** to perform secure transaction server **34** specific operations. To enable this, the server configuration files need to be changed so that

the web server **69** knows which transaction services are provided by the secure transaction system. In this way, whenever an account holder attempts to access a transaction service, the server will call upon the account holder access functions that are defined in the shared object **66** and the web server **69** will not process the request for transaction services until it receives permission to do so from these functions. The functions in the shared object **66** insure that the account holder is operating as a valid session. If it is not a valid session, the functions redirect the account holder to the login process so that a new session can be created for the account holder. Once there is an active session, the shared object **66** will grant permission to the web server **69** to process requests for transaction services and once the request has been processed, the shared object sends a message to the session manager **52** about a particular transaction so that the session manager can update its lists of transactions for the active session.

There are a number of account holder access common gateway interface programs (CGI'S) that are a part of the secure transaction server **34**, including a login CGI **68**. Any time an account holder is redirected by the system shared object **66** to login and start a new session, the login CGI gets executed. These CGI's communicate with the account holder software to authenticate the secure transaction server and send a command to force the account holder to login. When the CGI's get the login parameters sent by the account holder software **36**, they send a request to the session manager **52** to authenticate the account holder and start a new session. There is also a re-authentication CGI **70** that is provided. Once a session has been initiated, periodically the shared object **66** will redirect the account holder to get re-authenticated. The re-authentication CGI **70** communicates with the account holder software **36** to poll the account holder's machine for the hardware key **54**, and based upon the response, the re-authentication CGI's communicates with the session manager **52** to validate re-authentication and renew the account holder session.

The secure transaction server **34** also includes an online account holder application and activation CGI's **74** which allow a person to apply online for transaction services. The CGI's collect the application data and send it to the transaction clearinghouse **30** that updates the account holder access database. Also, for an existing account holder who is trying to apply for another account, the CGI's will communicate with the transaction clearinghouse to get the account data on the account holder in order to fill out as much of the application automatically as it can. The activation feature is for users who have been approved and are trying to access secure transaction services for the first time. The CGI's for activation insure that the account holder has properly installed the account holder software and then these CGI's will send a message to the transaction clearinghouse to activate the account holder so that these approved users can access the new service. A site administration CGI **76** is another component included for providing an HTML visual interface to define the account holder profile and administer the session manager **52** for that particular account holder profile.

The account holder software **36** is installed on the account holder's personal computer. This software enables a web browser **77** to access the transaction services **78** provided by the secure transaction server. The account holder software is a plug-in or control that adds secure transaction functionality **79** to standard browser software. The account holder software accepts messages from the web server **69** and takes actions as commanded by the secure transaction server such as making the account holder login, polling for the optional hardware key, encrypting the login parameters and sending it to the

secure transaction server. The account holder software also authenticates the server 34 before accepting any commands from it so that only authenticate servers can command the account holder software.

Referring to FIG. 5, the main function of the transaction clearinghouse database server 56 is to provide the database interface to the rest of the account holder access components. The transaction clearinghouse database server 56 contains the enterprise-wide account holder and transaction data warehouse. This database server is a SQL server that has an ODBC interface so that the clients can interact with it using ODBC. The processes and application that interact directly with the transaction clearinghouse database server 56 are the account holder authentication daemon 58, the transaction daemon 60, and the thin client transaction clearinghouse administration software 64.

Referring to FIG. 6, the account holder authentication daemon 58 interacts with the transaction clearinghouse database server 56, the session manager 52, the account holder application and activation CGI's 74, and any CGI's that use the API's provided by the secure transaction system, such as the credit card processing CGI's 80. In order to start a new session for a account holder, the session manager 52 sends an authenticate login (AL) message to the account holder authentication daemon 58, which queries the transaction clearinghouse database server 56 to find the appropriate account holder records in order to do the login validation. The result of this validation is sent back to the session manager 52 as an authentication response (AR) message.

The online application CGI's 74 interact with the account holder authentication daemon 58 to process an online account holder application. Normally, users fill out an online application form and submit it to one of the online application CGI's which will send all the application data in the form of an application (AP) message to the account holder authentication daemon. The daemon will verify and update the database with the application information and send back an application response (PR) message to the application CGI's indicating the status of the database update.

In cases where an existing account holder is applying for another account, the application CGI's 74 communicate with the account holder authentication daemon 58 to get the account holder information on the current account holder so that the application form can be filled automatically. In order to do this, one of the application CGI's 74 sends a verify application (VA) message to the account holder authentication daemon 58. The daemon will query the transaction clearinghouse database server 64 to verify the applicant and get the account holder information. Based on the query results, it will send a verification response (VR) back to the application CGI 74 which will contain the account holder information. The application CGI 74 will fill out the account holder part of the application form with this information. The account holder fills out the rest and submits the form that gets processed through the AP/PR message mentioned previously.

Once a user has been approved, the user needs to activate the account in order to access transaction services. This can be done online through the online activation CGI's 74. Typically, an approved user (i.e., an account holder) will have to login in order to access the online activation CGI 74, which in turn sends an AA (Activate Applicant) message to the account holder authentication daemon 58 with the approved user's login parameters. The daemon 58 will query the transaction clearinghouse database server 64 to validate this information, and based on the validation results, it will send back an activation response (AR) message to the online activation CGI.

For web applications that need credit card information on account holders, the account holder authentication daemon 58 provides an API to do so. This also assumes that the account holder has logged in successfully and has an active session, which means these web applications need to be secured. In order to obtain the credit card information, these web applications can send a CC (credit card) message to the account holder authentication daemon 58. The daemon will first validate the account holder and if the validation is successful, it will send back a credit response (CR) to the credit card processing web application 78 that includes the account holder's credit card information.

Referring to FIG. 7, the main task of the transaction daemon 60 is to update the transaction clearinghouse database server 56 with transaction data sent by the secure transaction server session manager 52. The transaction daemon 60 is an independent process listening for TCP requests on a specific, well-known TCP port. When a account holder session terminates, the session manager 52 will send a transaction session (US) message to the transaction daemon 60 that provides some generic information about the account holder's session and also the number of transactions in the session. This message is followed by a series of session transaction (ST) messages, where each transaction in that session is represented by a ST message. The transaction daemon 60 reads the US message and the following ST message(s), formulates SQL queries that will update all that data into the transaction clearinghouse database 56. The transaction daemon 60 will then send back a message confirmation (MC) back to the session manager 52 that indicates the status of the database update.

As shown in FIG. 8, the transaction clearinghouse administration software 64 is a thin client GUI web-based application for transaction clearinghouse database administration. This software runs on a computer with a web browser and communicates with the transaction clearinghouse database server 56. This application will typically be on the private network of an organization so that database access through the administration software 64 is restricted within the organization. The administration software 64 allows an administrator to define the particular transaction services that can be accessed by an account holder. It allows entering users as an account holder, approving and activating the account holder, and maintaining account holder profiles. It also provides inquiry screens to peruse transaction data. Also provided are table maintenance screens for the code tables in the database. The transaction clearinghouse servers preferably communicate with a database using open database connectivity (ODBC) drivers 81 most commonly over a TCP/IP network, and the transaction clearinghouse administration software 32 communicates with the database using an ODBC driver 81, most commonly over a TCP/IP or IPX network. As shown in FIG. 9, the account holder access shared object 66 is a binary module that combines with the web server 69 to provide system-specific function pointers to the web server. Thus, when the web server 69 is configured to protect transaction services using the system, it will call upon these system specific functions. These functions provide a variety of features ranging from redirecting an account holder to the login CGI's 68 to communicating with the session manager 52 to authenticate every request for transaction services. Whenever there is an incoming request from a web browser 77 including the account holder software 36 that attempts to access a transaction service, the web server 69 invokes the shared object 66. The shared object 66 calls a secure transaction system function that first looks for an active session ID in the HTTP headers. If it does not find the session ID, it will redirect the account holder to the login CGI's 68 in order to

**11**

initiate the login process. If it finds a session ID, it sends a check session (CS) message to the session manager **52** to validate the session ID. The session manager **52** will send the results of its validation in a session response (SR) message.

If the SR message has a SUCCESS status, the shared object **66** grants permission to the web server **69** to process the request for the account holder to access transaction services. At the end of processing this request, the shared object **66** calls another secure transaction system function that sends an end transaction (ET) message to the session manager so that the session manager **52** can log the end time for the specific web transaction. Periodically, the SR message will ask the shared object **66** to perform session re-authentication. At such times, the shared object **66** redirects the account holder to re-authentication CGI's **70**.

With the system architecture, transactions are protected on a directory level. A web master or a system administrator needs to determine which transactions are to be protected and make sure that all these transactions are organized in separate directories from unprotected transaction services. In this way, the web server configuration can be changed to protect these particular directories using the secure transaction system. Among other things, the configuration parameters also need to state where the session manager **52** is running and the port where it is listening for UDP requests. If there are multiple account holders being hosted from the same web servers **69**, it is very important to have their transaction services contained in separate directories, and also very important is to have separate copies of session managers **52** running for each account holder. This ensures that account holder authentication, authorization, and transaction tracking is done separately for separate account holders.

The secure transaction server session manager shown in FIG. 10 is an independent server process. It starts by reading configuration parameters from its configuration file, session-d.conf. It listens for requests on two different ports—one UDP, and one TCP. The UDP port communicates with the account holder access shared object **66** and the account holder access CGI's that reside on the same machine where the session manager **52** is running. The TCP port is for communication with the account holder access transaction clearinghouse daemons.

The session manager **52** maintains a binary tree list of all the active account holder sessions. For every session, it maintains a linked list of all the transactions for that session. As stated in the description of the shared object **66**, every time a web request comes in for a transaction service, the web server **69** will invoke the shared object **66**. The shared object **66** looks at the web server configuration files to determine which session manager **52** (hostname and UDP port number) to send its check session (CS) message. In processing a CS message, the session manager **52** will traverse its list of active sessions looking for the particular session ID, and sends the result of this search back in a session response (SR) message.

During login, the login CGI's **68** send an initiate session (IS) message to the session manager **52**, which will read the login parameters, and send an authenticate login (AL) message to the transaction clearinghouse account holder authentication daemon **58**. The session manager **52** will read the account holder authentication daemon's **58** authentication response (AR) and determine whether or not to create a new session entry, and sends a session response (SR) back to the login CGI's **68** indicating the result of the session initiation process.

While processing a CS message sent by the shared object **66**, periodically the session manager **52** will find that a particular session needs to be re-authenticated. In such instances,

**12**

the session manager **52** will respond back to the shared object **66** with a session response (SR) message that tells the shared object **66** to initiate the re-authentication process. The shared object **66** in turn invokes the re-authentication CGI's **70**. The re-authentication CGI's **70** perform the re-authentication task with the account holder software **36**, and sends the results in a renew session (RS) message to the session manager **52**. The RS message contains the newly encrypted digital ID optionally stored on the access media which is read by the hardware key **54** attached to the account holder's machine. The session manager **52** authenticates the digital ID by comparing it to the information it has in the session entry for the particular account holder. The results of this authentication are sent back to the re-authentication CGI **70** in a session response (SR) message.

During specific time intervals as set in the session manager **52** configuration, the session manager goes through its list of sessions and times out any idle sessions, flagging them as inactive. These are sessions that have not had an activity in the last n seconds, where n is a session manager configuration (REFRESH\_TIME) value. For each one of these inactive sessions, the session manager **52** initiates a process that will send all the transaction data collected for that session to the transaction clearinghouse's transaction daemon **60**. The process first reads the session-entry and sends a transaction session (US) message that will tell the transaction daemon **60** how many transaction entries will be sent for that session. The US message is followed by a series of session transaction (ST) messages where each ST message represents a transaction for that session. The process terminates after sending all the US and ST messages. The transaction daemon **60** will update the transaction clearinghouse database with all the transaction data, and sends a message confirmation (MC) message back to the session manager **52**. The session manager **52** determines which specific session the MC message is for, and deletes that session and its transactions from its list. If the MC message status is not successful, the session manager **52** tries to resend the transaction data. The number of retries is set in the session manager **52** configuration. If it is still unsuccessful, then the session manager **52** sends an e-mail to the system administrator indicating the error in transaction data update.

Another entity that the session manager **52** performs processing for is the site administration CGI's **76**. The specific operations provided are data recovery, data dump, and data restore features. During data recovery, the site administration CGI's **76** send a DR (data recovery) message to the session manager **52**. The session manager **52** will retry sending the transaction data for the session(s) specified in the DR message to the transaction clearinghouse's transaction daemon **60**.

During a data dump, the site administration CGI **76** sends a data dump (DD) message to the session manager **52** who makes a copy of all the active session data into a flat text file under the filename specified in the DD message. During a restore dump, the site administration CGI **76** sends a restore dump (RD) message to the session manager **52** who reads the dump file as named in the RD message and builds its list of sessions and transactions from the dump file data. To all these messages (DR, DD, RD), the session manager **52** sends a SR message back to the site administration CGI's **76** indicating the results of the particular operations whether they were successful or not.

Referring to FIG. 11, the login CGI's **68** is initiated when the shared object **66** redirects a account holder to login. It first sends a start login message to the account holder software **36** combined with the web browser **77** through the web server **69**.

The account holder software 36 then creates a random challenge and sends it to the login CGI's 68 for secure transaction server authentication purposes. The login CGI's 68 encrypts the secure transaction server's password using the challenge sent by the account holder software 36 and sends it back to the account holder software along with a login command and a new random challenge created by the login CGI 68. The account holder software 36 then authenticates the secure transaction server's password, and if it authenticates successfully, it will force the account holder to login. The login parameters obtained from the account holder and the hardware key 54 are encrypted using the challenge sent by the login CGI 68, and sent back to the login CGI.

The login CGI's 68 take the encrypted login parameters sent by the account holder software 36 and send an initiate session (IS) message to the session manager 52. The session manager 52 conducts the account holder verification with the aid of the transaction clearinghouse 30 and sends back a session response (SR) indicating if a new session entry was created. If SR status is successful, the login CGI 68 will put the session ID in the HTTP headers for re-authentication purposes.

As shown in FIG. 12, the re-authentication CGI's 70 are invoked by the account holder access shared object 66. The web server 69 sends a check login message to the account holder software 36 combined with the web browser 77 with a newly created challenge. In response to this message, the account holder software 36 polls the hardware key 54, reads the digital ID from the access media, and encrypts it using the challenge sent by the re-authentication CGI's 70, which is sent back to the re-authentication CGI 70 who will validate the information by sending a renew session (RS) message to the session manager 52. The session manager 52 validates the encrypted digital ID and sends back a session response (SR) message indicating the status of the re-authentication. If SR status is successful, the re-authentication CGI 70 redirects the account holder to the protected transaction services, otherwise they are directed to the login process.

Referring to FIG. 13, the online application process is initiated by a new user filling out an HTML application form and submitting it to the application CGI 74. If the user is an existing account holder, a separate link can be activated by the user that will automatically fill out the demographic part of the application form. When an existing account holder goes through this link, the account holder must login. The particular application CGI 74 will then send a verify application (VA) message to the account holder authentication daemon 58. The daemon 58 will first authenticate the account holder, and if the authentication is successful, it will send back the demographic information on the account holder in its verification response (VR) message. The application CGI 74 will fill out the HTML application form with the information in the VR message. For a user who is not an existing account holder, the user is required to go to the application form directly to manually fill out all the fields, and submit the form back to the web server 69.

When the application form is submitted to the web server 69, the application data is sent to another application CGI 74 who will send an application (AP) message to the account holder authentication daemon 58. The daemon 58 will verify all the application data and update the transaction clearinghouse database. The result of the database update is sent back to the application CGI 74 in an application response (PR) message. The application CGI 74 will then display the result of this process to the user on the web browser 77.

The application approval process can be conducted in a variety of ways. For account holders offering one-factor

authentication only, where a hardware key 54 is not used, a user can be instantly approved during the time of application, in which case the PR message contains the username, password, PIN assigned to the user. This information is immediately displayed back to the user so that the user can quickly proceed with the account holder activation process. Alternatively, another method is not approving the application immediately. Instead, a system administrator will perform additional processing of the application data to ensure that the user meets all the prerequisites of being an account holder. This could involve things like collecting payment, credit checks, etc. Once the requirements are met, the system administrator can approve the user using the transaction clearinghouse administration application software.

The result of the application approval process is that the user will now be assigned a unique account username and a password. If the account holder uses two-factor authentication, the approval process also involves assigning a unique digital ID to the user, and microcoding that digital ID into the access media read by the hardware key 54. All this information (username, password, PIN, digital ID), the user's hardware key and access media 54, and the account holder software 36 need to be made available to the approved user so that the user can successfully install the hardware key and account holder software 36 on the desktop, and proceed with the activation process.

The activation process is complete when the user becomes an account holder for a particular set of transaction services. Similar to the application process, this can be done through either online or through the account holder administration software 32. Online activation requires an approved user to install the account holder software on their desktop and visit the activation URL using the web browser 77. When the user clicks on the activation URL, the user must login. At this point, the approved user will use the username, password, PIN and the hardware key when using a two-factor authentication login. The activation CGI 74 takes all this information and sends an approve user (AU) message to the transaction clearinghouse's account holder authentication daemon 58. This daemon 58 will accept the AU message, and verify all the information with the approved user's information in the transaction clearinghouse database. If the verification is successful, the account holder authentication daemon 58 will create a new account holder record for the user if there is not already one, and also create a new account holder record for the particular account holder(s) for which the user was approved for. The result of this process is sent back to the activation CGI in an activation response (RA) message. If RA message status is successful, the activation CGI 74 will display a successful activation message to the account holder, and give the account holder an option to change their password if desired. Otherwise, the activation CGI 74 will display the error message explaining why application activation could not be conducted successfully.

A feature of the online application and activation process is the password change feature that can be made available as a separate link in a secured web site. This link must be protected by the system so that only valid account holders can use this feature. When this link is accessed, a password/PIN change form is displayed to the account holder where they type in the old and new passwords/PINs. Once this form is submitted, a password/PIN change CGI 82 will send a change password/PIN (CP) message to the account holder authentication daemon 58 in the transaction clearinghouse that will verify the account holder and the old password/PIN. If the verification is successful, the account holder authentication daemon 58 will make the password/PIN change in the transaction clearing-

house database. The status of this process is sent back to the password change CGI 82 in a password/PIN response (RP) response. Based on the RP message status, the password/PIN change CGI will display a message to the account holder indicating whether the password/PIN change was carried out successfully.

As shown in FIG. 14, the site administration CGI's 76 allows for the session manager configuration entries to be defined and maintained through an HTML interface. It also allows for the starting, stopping, and restarting of the session manager(s) 52. The specific operations provided by the site administration CGI's 76 that involve message interaction with the session manager 52 are the data recovery, data dump, and the data restore features. During a data recovery, the site administration CGI's 76 send a DR (data recovery) message to the session manager 52. The session manager will retry sending the transaction data for the session(s) specified in the DR message to the transaction clearinghouse's transaction daemon 60.

During data dump, the site administration CGI 76 sends a data dump (DD) message to the session manager 52 that makes a copy of all the active session data into a flat text file under a specified filename in the DD message. During restore dump, the site administration CGI 76 sends a restore dump (RD) message to the session manager 52, which reads the named dump file(s) from the RD message and builds a list of sessions and transactions from the dump file data. For any of these messages (DR, DD, RD), the session manager 52 sends a SR message back to the site administration CGI's 76 for indicating the results of success or failure for these particular operations.

FIGS. 4-14 described the software components of the preferred embodiment. The specific operations of the system will now be described in connection with the flow charts of FIGS. 15-20. In order to distinguish the present invention from the preferred embodiment in the web environment, the flowcharts use different terminology for the system components. The following table provides a cross reference between the flowchart components and the preferred embodiment.

FLOWCHART COMPONENTS	REFERRED EMBODIMENT ONTO WEB ENVIRONMENT
Client Application	Web browser
Client Messenger	a module of account holder software
Server Authenticator	a module of account holder software
Log-in interface	a module of account holder software
Access device interface	a module of account holder software
Client Cryptographer	a module of account holder software
Content Controller	a module of account holder software
Network transaction tracker	a module of account holder software
Server Application	Web Server
Communication Headers	HTTP headers
Client Authenticator	a module of Shared Object for Web Server
Transaction Monitor	a module of Shared object for Web Server
Log-in Enforcer	Log-in CGI's
Access device Validator	Re-authentication CGI's
Session Validator	a module of Session Manager
Session Initiator	a module of Session Manager
Session Terminator	a module of Session Manager
Authentication Server	Transaction clearinghouse Account holder authentication daemon
Transaction Data Server	Transaction clearinghouse Transaction daemon

Referring to FIG. 15, the flow chart illustrating the sequence of steps that occur during the start of a session is illustrated and begins with the account holder requesting access to a transaction service (block 100). The server appli-

cation forwards the request to the client authenticator (block 102). If the session ID is in the communication headers (block 104), the client authenticator sends a check session message to the session validator (block 106), and the session validator searches for a session entry in its list of active sessions (block 108). If the session ID is not in the communication headers (block 104), the client authenticator denies permission to the server application for servicing the account holder's request (block 110). Also, if the active session entry is not found (block 112), the session validator sends an unsuccessful session response to the client authenticator (block 114). However, if there was an active session entry found, a subroutine of transaction service and logging is initiated (block 116), which will be described later in conjunction with FIG. 17. If the client authenticator, on the other hand, denies permission to the server application (block 110) when the session ID is in the communication header (block 104) or after the session validator sends an unsuccessful session response (block 114), the server application invokes the login enforcer to make the account holder login (block 117). This results in a start login message being sent to the client messenger through the client application (block 118). The client messenger then sends a random challenge to the login enforcer through the server application (block 120), and the login enforcer encrypts the server application password with a client messenger challenger (block 122). The login enforcer then sends a login command in its encrypted password to the client messenger with a new random challenge of its own (block 124), and the client messenger then invokes server authenticator to authenticate server applications password (block 126). If the server authentication is successful (block 128), another subroutine of a login, account holder authentication and session initiation process is initiated (block 130), which will be described in conjunction with FIG. 16. If not, the client messenger displays a server authentication error message to the account holder (block 132), and the process is completed.

A flow chart of the login, account holder authentication, and session initiation subroutine is shown in FIG. 16, and indicated generally at 103. The client messenger first invokes a login interface to prompt account holder for a username, a password, and/or a PIN (block 140). The account holder then enters the username, the password, and/or the PIN (block 142), followed by the login interface requesting the hardware key interface to poll for the hardware key (block 144). If using two or three factor authentication, the hardware key interface reads the digital ID from the access media and sends it to the login interface (block 146). In the case of one factor authentication, the login interface assigns a blank digital ID for the login parameters. The login interface then sends the login parameters, including the username, password and digital ID to the client cryptographer (block 148). The client cryptographer encrypts the password and the digital ID using the challenge sent by the login enforcer and sends them to the login enforcer (block 150). The login enforcer then sends an initiate session message to the session initiator with the encrypted login parameters (block 152). The session initiator accordingly sends an authenticate login message to the transaction clearinghouse account holder authentication server (block 154), and the account holder authentication server accesses the account holder's information from its database and authenticates the login parameters (block 156). If using two or three factor authentication, this authentication involves the comparison of the digital ID, otherwise only username, password, and PIN are considered as login parameters. If the authentication was successful (block 158), the account holder authentication server sends a successful authentication response message to the session initiator

(block 160). The session initiator enters a new session entry for the account holder in its list of active session with a unique session ID (block 162). The session initiator also sends a successful session response to the login enforcer (block 164), followed by the login enforcer entering the account holder's new session ID in the communication headers for re-authentication purposes (block 166). The login enforcer also grants permission to service the account holder's request for secure transaction services (block 168), and proceeds to initiate the subroutine of transaction service and logging (block 116) shown in FIG. 17. However, if authentication is unsuccessful (block 158), the account holder authentication server sends an unsuccessful authentication response to the session initiator (block 172). The session initiator then sends an unsuccessful session response to the login enforcer (block 174). The login enforcer accordingly denies permission to the server application to service the account holder's request for transaction services (block 176), and the server application sends back an error response to the account holder (block 178).

The subroutine of the transaction service and logging process (block 16) is shown in FIG. 17. The session validator first enters a new transaction entry for the account holder's current session (block 180). The session validator then sends a successful session response to the client authenticator (block 182), and the client authenticator grants permission to the server application to service the account holder's request (block 184). The server application invokes the appropriate service function to enable the account holder to access the requested transaction services (block 186) and the transaction monitor sends an end transaction message to the session validator (block 188). The session validator updates the transaction entry with the transaction-specific information in the end transaction message (block 190).

In accordance with an important aspect of the present invention, the system is preferably adapted to periodically re-authenticate an active session to prevent unauthorized use by someone who no longer has the hardware key 54 connected to his computer. With respect to the re-authentication process, and referring to FIG. 18, the process begins with an account holder in an active session requesting a transaction service (block 200). The server application forwards the request to the client authenticator (block 202), and communication headers are screened to see if they have a session ID (block 204). If there is no session ID (block 204), the client authenticator denies permission to the server application to service the request (block 206) and the server application directs the account holder to the login enforcer to start a new session (block 208). If, however, the session ID is in the communication header (block 204), the client authenticator sends a check session CS message to the session validator (block 210).

From the CS message, the session validator searches for a session entry in its list of active sessions (block 212) and determines whether an activate session entry was found (block 214). If not, the session validator sends an unsuccessful session response to the client authenticator (block 216) and the client authenticator denies permission to service the request (block 206). The server application would again direct the account holder to the login enforcer to start a new session (block 208). If an active session is found (block 214), then the session validator checks for the time of the last polling of the account holder's machine to determine whether the hardware key 54 is present (block 218). The time duration is checked to determine if the preset time limit has been exceeded (block 220), and if it has not, then the system goes to the subroutine of the transaction service and logging step (block 170) (see FIG. 17). If the time duration has exceeded

the preset time limit, the session validator sends a session response to the client authenticator asking to poll for the account holder's hardware key attached to the account holder's computer (block 222). The client authenticator invokes the access device validator (block 224), and the access device validator then sends the check login message to client messenger with a new randomly generated challenge (block 226). The client messenger invokes the login interface (block 228), which in turn invokes the access device key interface (block 230). The access device interface polls the account holder's machine for the hardware key 54 (block 232) and reads the digital ID from the access media. If the digital ID is successfully read (block 234), the program implements a session renewal (block 236), which is shown in FIG. 19. If the digital ID is not successfully read (block 234), the access device interface sends an error message to the login interface (block 238) and the login interface generates an error message to the client messenger (block 240). The client messenger then sends an unsuccessful polling message to the access device validator, which redirects the account holder to the login enforcer (block 242).

With respect to the session renewal and referring to FIG. 19, the access device interface reads the digital ID of the access media and submits it to the login interface (block 250), which in turn submits the digital ID to the client cryptographer (block 252). The client cryptographer encrypts the digital ID using the challenge sent by the access device validator and sends the encrypted digital ID 10 to the access device validator (block 254), which then sends a renew session message to the session validator with the encrypted digital ID (block 256). The session validator finds account holder session entry and validates the encrypted digital ID (block 258) and determines whether the validation was successful (block 260). If not (block 260), the session validator sends an unsuccessful session response to the access device validator (block 262), and the access device validator redirects the account holder to the login enforcer to start a new session (block 264). If validation was successful (block 260), the session validator updates the session entry's time of last re-authentication (block 266) and sends a successful session response to the access device validator (block 268). The access device validator grants permission to the server application to process the account holder's request for transaction services (block 270), and then proceeds to the transaction service and logging step (block 116) (see FIG. 17).

With respect to session termination and referring to FIG. 20, the first step is to begin with the first session entry of a session list (block 280) and the session terminator checks the difference between the current time and the time of the last request (block 282). If the time difference did not exceed the idle time limit (block 284), the program determines whether the first session entry is the last session entry in the session list (block 286). If so, the session is terminated (block 288). If it is not the last session entry in the list (block 286), the program fetches a next session entry in the list (block 288) and return to block 282. If the time difference did exceed the idle time limit (block 284), the session terminator tags the session entry as inactive (block 290) and sends all session transaction data to the transaction clearinghouse's transaction data server (block 292). The transaction data server updates the transaction clearinghouse database with the session transaction data (block 294), and the program determines whether the update was successful (block 296). If not, the transaction data server sends an unsuccessful message confirmation to the session terminator (block 298), which prompts the session terminator to send an error message to the system administrator (block 300). If the update was successful (block 296), the transaction

19

data server sends a successful message confirmation to the session terminator (block 302) and the session terminator then removes the session entry from the session list (block 304).

In accordance with another important aspect of the present invention, and referring to FIG. 21, a hardware token access device 450 for use as the hardware key 54 is shown in the illustrated functional block diagram. The access device 450 is an external hardware device, such as the iKey 1000 USB Smart Token device manufactured by Rainbow Technologies of Irvine, Calif. The hardware token access device 450 preferably connects to the USB port of the account holder's personal computer. The major function of the hardware token access device 450 is to uniquely identify a account holder that desires to access the transaction services and computer resources of an untrusted network, such as the Internet. It is used in conjunction with the username, password, and/or PIN to provide two factor authentication. Generally, two factor authentication provides that something is known (e.g., the username and password) and something is held (e.g., the physical hardware token that is attached to the computer or built into the computer). While the Rainbow iKey 1000 USB Smart Token is the preferred embodiment for the hardware token access device 450, it should be understood that the two factor authentication could be provided by some other physical device, such as a credit card, a key, an ATM card, or the like which is known to have been assigned and given to a specific person.

In FIG. 21, the hardware token access device 450 includes a port interface 480, which provides an interface to support the personal computer of the account holder 36. Such may include, for example, USB, parallel, serial and/or keyboard ports. The access device 450 is transparent to the personal computer interface being utilized and does not prohibit the personal computer interface from being used in a normal fashion. In the Rainbow iKey 1000 Smart Token, it is preferred that the hardware token be connected to the USB port. The hardware token also includes a data bus buffer 482, which provides a minimum internal data bus of eight bits regardless of the port interface configuration. A read/write control logic block 484 manages all the internal and external transfer of data controlled status, while a control register 486 initializes the functional configuration of the access device 450. A status register 488 contains the result of the last operation performed using the control register 486 on the read/write control logic 484. A message digest encryption 490 is used to encrypt both a nonvolatile general purpose memory 492 during memory read and password read operations. The message digest encryption engine 490 accepts a seed value from the port interface 480 that can be used to uniquely encrypt the data being read. The memory 492 contains a minimum of 1024 bytes of data that can be used for storage of information for personally identifying the account holder. This information can include, but is not limited to a digital certificate. A password register 494 accepts a minimum of a 64 bit password from the port interface 480, and a password comparator 496 performs a logical XOR on the contents of the password register in the contents of the nonvolatile password memory 492. When the contents of the password register 494 are equal to the contents of the nonvolatile password memory 498, several operations can be performed, such as reading the nonvolatile general purpose memory, read the encrypted nonvolatile password memory, writing the nonvolatile general purpose memory, writing the nonvolatile password memory and writing a seed value to the message digest encryption engine. The nonvolatile password memory contains a mini-

20

mum of a 64 bit password. The password is set to a known default value at the time of manufacture but can be reprogrammed at any time.

In accordance with another important aspect of the present invention, and referring to FIG. 22, a magnetic card reader access device in use with an access media 54 is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and indicated generally at 499. A magnetic card is a plastic card with a strip of magnetic recording tape adhered to the back of the card. The magnetic recording strip has three tracks that can be used for storing and retrieving data. In the context of the preferred embodiment, the magnetic card 500 is the preferred access media containing a digital ID. Magnetic stripe cards, which typically only store about 1 kilobyte of data (compared with 8, 16, or 32 KB in smart cards), do not have a CPU and rely on the card reader, the PC to which it's attached, or a remote computer accessed via modem to perform transaction processing. Magnetic card technology is widely utilized in Point of Sale (POS) terminals, Automated Teller Machines (ATM), ticketing, card issuing, transportation, and access control.

Two types of devices, a reader and a terminal can read magnetic cards. A reader is interfaced to a personal computer for the majority of its processing requirements, while a terminal is a self-contained processing device. Magnetic card readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, parallel ports, infrared IRDA ports and keyboards. Terminals have their own operating systems and in addition to reading a magnetic card typically support other functions such as network connectivity, transaction printing, and keypad entry. Both terminals and readers are considered access devices 501 in the context of the preferred embodiment.

For example, a magnetic card reader can be attached to a personal computer (PC) and serves the role of an access device. The magnetic card reader connects in-line between a PC and its keyboard. The magnetic card reader is intended to remain virtually invisible to both the PC and the keyboard until a magnetic card is read. When a magnetic card is read, the magnetic card reader takes over the interface to the PC and sends card data using the same scan codes used by the keyboard. These scan codes are routed to the account holder software 36. Magnetic card readers also support the operation of a keypad that can be used to enter one or any combination of username, password or PIN codes in addition to the digital ID read from the access media by the access device.

In accordance with another important aspect of the present invention, and referring to FIG. 23, a smart card reader access device in use with an access media is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and indicated generally at 502. A smart card is a type of plastic card embedded with a computer chip that stores and transacts data between users. This data can contain several digital IDs that are stored and processed within the card's chip, either a memory or a microprocessor. The card data is transacted via a reader that is part of a computing system. Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart cards protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Within the context of the preferred embodiment, a smart card 503 is considered access media.

Two types of devices, a reader and a terminal can read smart cards. A reader is interfaced to a personal computer for the majority of its processing requirements, while a terminal is a self-contained processing device. Both are considered

access devices in the context of the preferred embodiment. Both the terminals and the readers read and write to smart cards. Readers come in many forms and in a wide variety of capabilities. Smart card readers that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports, infrared IRDA ports and keyboards are presently available. Smart card terminals have their own operating systems and typically support other functions such as reading a magnetic card, network connectivity, transaction printing, and keypad entry. Both the terminals and the readers are considered access devices 504 in the context of the preferred embodiment.

Smart cards have the tremendous advantage, over their magnetic stripe ancestors, of being able to execute cryptographic algorithms locally in their internal circuitry. This means that the user's secrets (be these PIN codes or keys) never have to leave the boundaries of the tamper-resistant silicon chip, thus bringing maximum security to the overall system where the cards are used. Smart-cards contain special-purpose microcontrollers with built-in self-programmable memory and tamper-resistant features intended to make the cost of a malevolent attack more than any benefits gained from the attack. Smart Card readers can also support the operation of a keypad that can be used to enter one or any combination of username, password or PIN codes in addition to the digital ID read from the access media by the access device.

In accordance with another important aspect of the present invention, and referring to FIG. 24, a biometric identification reader access device in use with an access media is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and generally indicated 505. As organizations search for more secure authentication methods for user access, e-commerce, and other security applications, biometrics is increasingly gaining attention in the marketplace. A biometric is one of the most secure and convenient authentication tool. It cannot be borrowed, stolen, or forgotten and is practically impossible to forge. Biometrics measure an individuals' unique physical or behavioral characteristics as a way to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics. Behavioral characters include signature, voice (which also has a physical component), keystroke pattern, and gait.

A biometric system works by capturing the chosen biometric with a biometric reader. The reader converts the biometric into a digital identification that is stored in a local repository for comparison during authentication. In the case of the preferred embodiment, the biometric reader 506 is equivalent to the access device; the biometric identification data 507 is equivalent to the digital ID created when the access device reads the fingerprint 508 access media; and the local repository that stores the biometric identification data can be the transaction clearinghouse. When logging into the secure transaction system, the account holder would have the chosen biometric (e.g., access media—fingerprint, palm, etc.) scanned by the biometric reader 506, forwarded to the clearinghouse using the previously described log-in process (FIGS. 15-20). The digital ID created by the biometric data would be compared to the digital ID already stored in the transaction clearinghouse for authenticity. It is also possible in the preferred embodiment to combine the digital ID created by the biometric scan to be supplemented with one or any combination of username, password, or PIN in addition to the digital ID read from the access media by the access device. Biometric identification can be also combined with smart cards or magnetic cards in the preferred embodiment.

In accordance with another important aspect of the present invention, and referring to FIG. 25, a secure central processing unit (CPU) in use with an access media is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and indicated generally at 509. In order to secure the CPU, a trusted subsystem must be inserted into the standard personal computer platform. The trusted subsystem is then able to extend its trust to other parts of the whole platform by building a 'chain of trust' where each link extends its trust to the next one. In this way, the secure CPU subsystem provides the foundation for a fully trusted platform and a basis for extending trusted computing across system and network boundaries.

The root of trust is a small hardware device called a Trusted Platform Module (TPM) 510. The TPM 510 is basically a secure controller that provides features like secure memory, cryptographic sign/verify, and an immutable key pair used to generate anonymous identities. In the preferred embodiment, the CPU and its associated platform 511 is the access device and the secure memory of the TPM 510 preferably acts as the access media and holds several types of unique digital IDs. Together they provide secure CPU functionality and provide all the functions of the account holder's PC. Another important feature of the TPM 510 is the possibility of producing random numbers. The TPM 510 can create digital signatures using the random number generator as the source of randomness required by the digital ID generation process. In order to generate a unique digital ID, each single TPM 510 has a unique key that identifies the TPM.

With these capabilities, the TPM 510 is able to produce a statistically unique digital fingerprint of the PC's basic input/output system (BIOS) firmware at boot time. This fingerprint is also called an integrity metric or cryptographic digest. Once this metric is available, it is saved in the TPM's secure memory location. During the PC boot process, other integrity metrics are collected from the PC platform, for instance, fingerprints of the boot loader and the operating system itself. Device drivers may be hashed; even hardware like PCI cards can be detected and identified. Every metric of the TPM 510 is concatenated to the already available metrics. This generates a final metric, which provides a unique digital ID for the PC.

The digital ID can also be used to encrypt other unique digital identification including account numbers, digital certificates, etc., and store the results in the protected storage of the TPM. The protected storage of the TPM is essentially non-volatile storage that has a means of access control. This access control determines which entities (e.g., user, programs, etc.) have permission to read, write, modify, and update the secure memory of the TPM. It is assumed that protected storage has some form of access control protocol that is used to protect against certain kinds of attack.

A distributed architecture of the system software enabling multiple web servers 69, each of which may host their own copy of a server 34 to communicate and interact with one or more transaction clearinghouses 30 is shown in FIG. 26. As shown in FIG. 26, there are multiple servers 69 residing in a geographically distributed manner on the Internet, each one of them with their own copy of a secure transaction server. The transaction clearinghouse 30 contains the enterprise wide account holder database, the transaction and demographics data warehouse, and controls the authentication and authorization of account holders on all the web servers 69.

When an account holder attempts to access a transaction service from any secure transaction enabled web sites, the respective server 69 for that web site will need to authenticate the account holder. In order to perform account holder

authentication, the secure transaction server will need to interact with the system transaction clearinghouse 30 by establishing and maintaining a communication line between itself and the transaction clearinghouse. The information transmitted on this communication line is encrypted using a public/private key mechanism so that only authentic servers and an authentic transaction clearinghouse can communicate with each other. The server 69 also implements the same mechanism in sending transaction data to the transaction clearinghouse's data warehouse.

The other secure transaction servers interact with the transaction clearinghouse 30 in the same manner. Thus a transaction service can host several geographically distributed secure transaction enabled web sites. Once an account holder is authenticated at one of the system enabled web sites, that account holder can access other likewise enabled web sites transparently using the same username, password, PIN combination, and the optional digital ID read from the access media by the hardware key 54, without having to again provide their username, password, PIN, and optional digital ID thus creating a single sign-on scenario where transaction services and computer resources can be accessed from a multitude of sources. All the transaction data generated by the account holder on all these different enabled web sites will be reported back to the transaction clearinghouse, regardless of how the account holder accesses the different enabled web servers 69. In the configuration of FIG. 26, the same transaction clearinghouse 30 was controlling all the secure transaction servers. However, the distributed architecture can be further extended to allow multiple secure transaction servers to interact with multiple transaction clearinghouses 30, which is shown in FIG. 27.

FIG. 27 shows multiple transaction clearinghouse two transaction clearinghouses shown), specifically a transaction clearinghouse A in Omaha and a transaction clearinghouse B in Chicago. Each transaction clearinghouse contains the business rules for account holder services, enforced by the individual transaction clearinghouse's enterprise wide account holder database. Assume that account holder "a" is registered with transaction clearinghouse A, and account holder "b" is registered with transaction clearinghouse B. Each secure transaction server 69 can provide secure transaction services for account holders from more than one transaction clearinghouse. For example, server 1 in Boston can provide secure transactions services to account holder A and account holder B even though they are registered at different transaction clearinghouses. In this case, the secure transaction server 1 in Boston is doing all the authentication, authorization and transaction data updates for account holder A through transaction clearinghouse A, and account holder B through transaction clearinghouse B. This scenario fits perfectly for a secure transaction service provider who wants to provide hosting services for several customers. The provider can run a web site with a copy of the secure transaction server, and host different transaction services through the secure transaction server, where different transaction clearinghouses are controlling different transaction services.

This also presents the possibility of transaction clearinghouses forming alliances with one another. For instance, in our example above, let's suppose transaction clearinghouse A and transaction clearinghouse B form a joint agreement that they will let each other's account holders access each other's account holder services, and each transaction clearinghouse will pay a share of the dividend to the other based on transaction volumes. In order to do this, system servers will need to be configured to perform authentication from both transaction clearinghouses. As a result, an account holder who is

registered with transaction clearinghouse A can access account holder services that fall under transaction clearinghouse B.

With regard to the case of server 1 hosting account holders A and B, since now an account holder registered with transaction clearinghouse A can also access account holder services that fall under transaction clearinghouse B, account holder "a" should be able to access account holder B through server 1. In order to do this, the server 1 will need to change its configuration so that it is able to separate transaction clearinghouse A account holders from transaction clearinghouse B account holders. When account holder "a" tries to access transaction services, secure transaction server 1 will interact with transaction clearinghouse A to do authentication, and if it is account holder "b", secure transaction server 1 will interact with transaction clearinghouse B.

However, the transaction data for a particular account holder will be sent to the transaction clearinghouse that owns the account holder. So even if account holders from transaction clearinghouse A can now access account holder B, all their transaction data will still be sent to transaction clearinghouse B. Thus, all of account holder "a" is transaction data regarding account holder B and go to transaction clearinghouse B. In this way, transaction clearinghouse B knows how many account holders from other transaction clearinghouses have accessed account holders that belong to transaction clearinghouse B, and based on that data, transaction clearinghouse B will be able to charge other transaction clearinghouses.

In accordance with another aspect of the present invention, the manner in which messages are sent among the various components will now be described in connection with the preferred embodiments of the programs that are utilized by the system. In this regard, the following is a listing of the software products that are part of the preferred embodiment of the present invention. The documents identified are specifically incorporated by reference.

#### Account Holder Database

##### Product: Sybase SQL Server XI

Installing Sybase SQL Server for Microsoft Windows NT  
Sybase SQL Server Release 11.0.x

Document ID: 34714-1101-02

Last Revised Mar. 6, 1996

##### Introducing Sybase SQL Server for Microsoft Windows NT

Sybase SQL Server Release 11.0.x

Document ID: 31965-1101-02

Last Revised Feb. 10, 1996

##### Configuring and Administering Sybase SQL Server for Microsoft Windows NT

Sybase SQL Server Release 11.0.x

Document ID: 36446-1101-02

Last Revised Feb. 22, 1996

##### Installing Sybase Products on Sun Solaris 2.x (SPARC)

Open Client/Server Release 11.1.x

Document ID: 35075-1100-03

Last Revised Sep. 10, 1996

##### Open Client/Server Configuration Guide for UNIX

Open Client/Server Release 11.1.x

Document ID: 35831-1100.quadrature.02

Last Revised Aug. 21, 1996

##### Open Client/Server Programmer's Supplement for UNIX

Open Client/Server Release 11.1.x

Document ID: 35456-1100-04

Last Revised Aug. 23, 1996

**25**

Sybase SQL Server Utility Programs for UNIX  
 Sybase SQL Server Release 10.0  
 Document ID: 30475-01-1000-04  
 Change Level: 1  
 Last Revised Feb. 1, 1994

Sybase SQL Server System Administration Guide  
 Sybase SQL Server Release 10.0  
 Document ID: 32500-01-1000-03  
 Change Level: 3  
 Last Revised Jun. 17, 1994

Sybase SQL Server Reference Manual: Volume 1 Commands, Functions, and Topics  
 Sybase SQL Server Release 10.0  
 Document ID: 32401-01-1000-03  
 Change Level: 2  
 Last Revised Jun. 17, 1994

Sybase SQL Server Reference Manual: Volume 1 System Procedures and Catalog Stored Procedures  
 Sybase SQL Server Release 10.0  
 Document ID: 32402-01-1000-03  
 Change Level: 2  
 Last Revised Jun. 17, 1994

Sybase SQL Server 11 Unleashed  
 by Ray Rankins, Jeffrey R. Garbus, David Solomon, and Bennett W McEwan  
 ISBN # 0-672-30909-2  
 Library of Congress Catalog Card # 95-72919  
 Sams Publishing, 201 West 103rd Street, Indianapolis, Ind. 46290  
 Copyright© 1996

Sybase Developer's Guide  
 by Daniel J Worden  
 ISBN #0-672-30467-8  
 Library of Congress Catalog Card # 93-87172  
 Sams Publishing, 201 West 103rd Street, Indianapolis, Ind. 46290  
 Copyright © 1994

ODBC Driver

Intersolv DataDirect ODBC Drivers  
 October 1995  
 9420 Key West Avenue  
 Rockville, Md. 20850  
 MA-ODBC-211-DREF

Intersolv DataDirect ODBC Drivers Installation Guide  
 Microsoft Windows, Microsoft Windows 95, Microsoft Windows NT, and OS/2  
 October 1995  
 9420 Key West Avenue  
 Rockville, Md. 20850  
 MA-ODBC-211-INST

Intersolv ServiceDirect Handbook  
 Fourth Edition 11/95  
 Copyright© 1995  
 Intersolv, Inc.  
 9420 Key West Avenue  
 Rockville, Md. 20850  
 QCS95-S-0231

Inside ODBC by Kyle Geiger  
 ISBN # 1-55615-815-7  
 Library of Congress Catalog Card # 95-18867  
 Microsoft Press  
 Copyright © 1995

Server Application (Web Server)  
 Product: Netscape Enterprise Server

**26**

Netscape Enterprise Server Version 2.0 Administrator's Guide  
 Copyright © 1996  
 Netscape Communications Corporation  
 5 501 East Middlefield Road  
 Mountain View, Calif. 94043  
 802-7610-10

Netscape Enterprise Server Version 2.0 Programmer's Guide  
 Copyright© 1996  
 Netscape Communications Corporation  
 10 501 East Middlefield Road  
 Mountain View, Calif. 94043  
 802-7611-10

Client Application (Web browser)  
 Product: Netscape Navigator  
 Netscape Navigator Gold Authoring Guide  
 Copyright © 1996  
 Netscape Communications Corporation  
 15 501 East Middlefield Road  
 Mountain View, Calif. 94043  
 802-7612-10

Using Netscape  
 ISBN # 0-7897-0211-8  
 Library of Congress Catalog #95-67809  
 Copyright © 1995  
 Que Corporation  
 20 201W.103rd Street  
 Indianapolis, Ind. 46290

Hardware Key  
 Product: iKey 1000 Smart Token (Hardware Token)  
 Rainbow Technologies, Inc.  
 25 50 Technology Drive  
 Irvine, Calif. 92618

Magtek  
 Product: Mag-Wedge Reader (Magnetic Card Reader)  
 Magtek  
 30 20725 South Annalee Avenue  
 Carson, Calif. 90746

Product: GemPC430 (Smart-Card Reader)  
 Gemplus Corporation  
 35 3 Lagoon Drive  
 Redwood City, Calif. 94065-1566

Product: FIU/SS2K (Fingerprint Biometric Reader)  
 Sony Electronics, Inc.  
 40 1 Sony Drive  
 Park Ridge, N.J. 07656-8002

Product: TPM (Trusted Platform Module—Secure CPU)  
 Infineon Technologies North America Corporation  
 45 1730 North First Street  
 San Jose, Calif. 95112

The secure transaction system (STS) is the preferred embodiment of the present invention in the web environment. The following table lists the STS software components as they relate to the present invention:

	Preferred Embodiment Component	STS software component
60	Transaction clearinghouse user authentication daemon	userauthd
	Transaction clearinghouse transaction daemon	transactiond
	Transaction clearinghouse administration software	ch_admin.exe
	STS Server Session Manager	sessiond
	STS shard object for Web server	sts.so
65	STS log-in CGI's	start_login.cgi login.cgi vrfypswd.cgi

-continued

		PARAMETER	DESCRIPTION
STS re-authentication CGI's	check_key.cgi verify_key.cgi	logdir	Absolute pathname specification of the directory which this daemon is to create its log files in. Two instances of the same daemon type (e.g., userauthd) cannot log to the same directory. The daemon will not start up if it is un-able to write to the directory.
STS online application CGI's and HTML	application.html application.cgi account_holder.cgi verify_applicant.cgi	service	Specifies the TCP port number which the daemon is to use to listen for requests. This can be a numeric or alphanumeric entry. If the entry is alphanumeric, there should be a corresponding entry in the/etc/services/file.
STS online activation CGI's	activate.cgi check_activate.cgi	10	
STS password change CGI's	pswd_chg_form.cgi chg_pswd.cgi add_profile.cgi	dbserver	The name of the database server to connect to. This entry should correspond to an entry in the database server interface file.
STS Site Administration CGI's	del_subs.cgi srvcfg.cgi admin_subs.cgi profile.cgi stadmin.cgi chng_srcfg.cgi data_dumprestore.cgi	15	The name of the database to use. A database server can control many databases.
	smgr_restart.cgi upd_profile.cgi data_recovery.cgi smgr_start.cgi upd_subs.cgi del_profile.cgi smgr_stop.cgi	dbname	The name of the database user to use when connecting to the database. Database users can be used to control what processes (or daemons) can connect to the database and also what permissions they have when they connect.
	STS Client Plug-in STS ActiveX component	20	Typically all transaction clearinghouse components will use the same database server name, database name, database username and hence database user password entries in their configuration files.
STS Account holder software		25	The password to use for the above database user. The file permissions for this configuration should be set according knowing that it contains a database username and password.

Following is a description how these STS components can be configured, initialized, and how their day-to-day operation can be monitored. It should be understood that the component names used in these descriptions are specific to STS, and the procedures described to perform the day-to-day operation are specific to STS components, more so as an example of the preferred embodiment of the present invention in the web environment.

With respect to the configuration files that are necessary for operating the various software components of the system, each component has its own configuration file as shown below:

Daemon/Server	Configuration Filename	PARAMETER	DESCRIPTION
User Authentication	userauthd.conf	logdir	Absolute pathname specification of the directory which this daemon is to create its log files in. Two instances of the same daemon type (e.g., transactiond) cannot log to the same directory. The daemon will not start up if it is unable to write to the directory.
Transaction	transactiond.conf	service	Specifies the TCP port number which the daemon is to use to listen for requests. This can be a numeric or alphanumeric entry. If the entry is alphanumeric, there should be a corresponding entry in the/etc/services/file.
Session Manager	sessiond.conf	40	
Web Server	magnus.conf obj.conf mime.types	45	The name of the database server to connect to. This entry should correspond to an entry in the database server interface file.

Each daemon accepts the name of its configuration file as a command line argument when starting the daemon. The format of the command line is:

<daemon name><configuration file>.

The transaction clearinghouse daemons can be started by using standard shell scripts.

For the account holder authentication daemon userauthd.conf), the following configuration files apply:

For the transaction daemon (transactiond.conf), the following configuration files apply:

Parameter	Description
SESSIOND_UDP_PORT	Specifies the UDP port which the session manager will use to list for requests from CGI programs.
SESSIOND_TCP_PORT	Specifies the TCP port which the session manager will use to listen for replies from the transaction clearinghouse.

For the session manager (sessiond.conf), the following configuration files apply:

Parameter	Description
SESSIOND_UDP_PORT	Specifies the UDP port which the session manager will use to list for requests from CGI programs.
SESSIOND_TCP_PORT	Specifies the TCP port which the session manager will use to listen for replies from the transaction clearinghouse.

-continued

Parameter	Description
TRANSACTION_CLEARINGHOUSE_HOST	The UNIX host name that the transaction clearinghouse server is running on. When the session manager communicates with the transaction clearinghouse, this entry forms part of the address.
TRANSACTION_CLEARINGHOUSE_PORT	This entry specifies the TCP port which the session manager should use when communicating with the transaction clearinghouse transaction daemon. The session manager uses this entry and the TRANSACTION CLEARINGHOUSE_HOST entry to build the complete address for the transaction daemon. This port number should match the port number defined in the service entry of the transaction daemons configuration file.
TRANSACTION_CLEARINGHOUSE_URL_PORT	This entry specifies the TCP port which the session manager should use when communicating with the transaction clearinghouse URL tracking daemon. The session manager uses this entry and the TRANSACTION CLEARINGHOUSE_HOST entry to build the complete address for the URL tracking daemon. This port number should match the port number defined in the service entry of the URL tracking daemons configuration file.
TRANSACTION_CLEARINGHOUSE_AUTH_PORT	This entry specifies the TCP port that the session manager should use when communicating with the transaction clearinghouse account holder authentication daemon. The session manager uses this entry and the TRANSACTION CLEARINGHOUSE_HOST entry to build the complete address for the account holder authentication daemon. This port number should match the port number defined in the service entry of the account holder authentication daemons configuration file.
COMPANY_NO	Unique ID assigned to each company defined with the secure transaction server system.
ACCOUNT HOLDER_ID	Unique ID assigned to each account holder defined for a company in the secure transaction server system.
KEYCHECK_INTERVAL	The number of seconds that will elapse before the secure transaction server asks the browser to check for the existence of the access device.
REFRESH_TIME	The amount of time (in seconds) that must expire without any session activity before a session is considered inactive and terminated.
SESSION_REFRESH_INTERVAL	The amount of time (in seconds) that must elapse with no new connection requests to the secure transaction server, which will cause the secure transaction server to stop listening for incoming connections and go examine its internal session table to see if any sessions have become idle (refresh time has expired for the session). It will clean up idle sessions and resume listening for incoming connection requests.
LOCAL_TRANSACTION_TRACK	Indicates if the transaction tracking data is stored locally as well as being sent to the transaction clearinghouse for storage. Valid entries are YES or NO.
MAX_RESEND_NO	If the secure transaction server does not get a confirmation message back from the transaction clearinghouse for information it sent to the secure access transaction clearinghouse, the secure transaction server will resend the data until we get a confirmation message or until the maximum times to resend transaction data has been exceeded.
ADMIN_EMAIL_ADDR	When an event occurs that requires intervention from an administrator, notification is sent to this email address.
MAIL_BIN	Absolute filename specification of the program to use to send email notification to the person defined in ADMIN_EMAIL_ADDR.
TRANSACTION	This defines the granularity of the transaction data that the session manager records about a session. There are two valid entries: SESSION or TRAN. TRAN indicates that the session manager should record information about every transaction that occurred in a session. SESSION indicates that only information regarding the session should be stored, i.e., session start and end times, account holder ID,

-continued

Parameter	Description
LOCAL_AUTHENTICATION	number of transactions that occurred in session manager. Indicates if account holder authentication should be performed against a local database as opposed to the transaction clearinghouse database. Valid entries are YES or NO. YES indicates that authentication should be performed locally, while NO indicates the opposite.
RUNTIME_DIR	This is the default directory for the secure transaction server. Here is where the secure transaction server will create log files and other dynamic run time files required for successful operation.

For the web server (magnus.conf), in order that the system shared object 66 component works correctly with the web server, the following changes need to be made to the magnus.conf file:

---

```
# load the account holderaccount holder access specific NSAPI functions
#
Init fn=load-modules shlib=/usr/ns-home/bin/load_modules/sts.so
funcs=init-sts,restrict-by-sts,log-end,restrict-by-rpa
#
#call init-sts to initialize sts server specific NSAPI
#variables
#
Init fn=init-sts
Sm_host=localhost
login_url=http://10.199.199.7/cgi-bin/gatekpr/login.cgi
keycheck_url=http://10.199.199.7/cgi-bin/gatekpr/check_key.cgi
smerr_url=http://10.199.199.7/gatekpr/session_err.html
```

---

It should be noted that all the <variable>=<value> pairs listed above should appear on the line beginning Init if and should be separated with spaces. Each variable/pair value was listed on a separate line to aid clarity.

The following describes the meaning of each of NSAPI variables:

Sm\_host: hostname or the IP address of the machine hosting session manager daemon(s)

login url: URL for the account holderaccount holder access login CGI

keycheck\_url: URL for account holderaccount holder access re-authentication CGI

smerr\_url: URL for error HTML for session manager errors (configurable)

For the web server (obj.conf), for each directory protected by the secure transaction system, the following entries need to be inserted in obj.conf:

---

```
<Object ppath="/usr/ns-home/htdocs_unsecure/demosite/*">
PathCheck fn="restrict-by-sts"
log_head="prism_login.txt"
session_port="50420"
trailer="prism_tail.txt"
err_head="prism_err.txt"
digest="5"
AddLog fn="log-end"
</Object>
```

---

Once again, each entry was placed on a separate line for clarity but when adding them to the configuration file all the entries should be on the same line, separated by spaces.

15 The variable meaning is as follows:  
log\_head: text file containing the HTML header tags for the login page

20 session\_port: session manager's port number  
trailer: text file containing the HTML trailer tags for login page and error pages

err\_head: text file containing the HTML header tags for error pages  
digest: message digest type to use for one-time-password encryption (4-MD4; 5-MD5)

25 For the web server configuration file (mime.types), one line needs to be added to the mime.types configuration file. The line is:

30 type=application/x-protect exts=pro  
The positioning of the new line within the configuration file is not important. Adding this line enables any file with the extension pro to automatically invoke the client side software to process the file.

35 With respect to routine operating procedures, there are general guidelines for the orderly start up and shutdown of the system of the present invention. To start up the system, there are a sequence of activities that are involved. First, each server should be configured through its configuration files. Each of 40 the transaction clearinghouse servers is started by a series of shell strips, which in a typical installation, will be in the directory named /usr/local/sts/transaction clearinghouse. The /usr/local part of the previous pathname was the directory specified at installation time. The scripts are named start\_userauthd.sh, start\_transactiond.sh and start\_urtrackd.sh. After the scripts are executed, the PS-EF command is used to check if the following processes exist: userauthd, transactiond and urtrackd. The next step is to start up the database server which requires login as the account holder sybase. This 45 50 login will have an environment variable called SYBASE which defines what directory SYBASE was installed to. It is necessary to move to the directory \$SYBASE/bin. For each database server to be started, there is a file called RUN\_<SERVER\_NAME>. If two database servers called STS and STS\_backup were created during the installation, the start up files would be called RUN\_STS and RUN\_STS\_BACKUP. This start up file should be used in conjunction with the startserver program. The exact syntax is: startserver {f<startup files>}. To continue the example from above, the 55 command would be: startserver -fRUN\_STS-fRUN\_STS\_BACKUP.

With respect to the session manager, it can be started by a shell script and there will be one instance of the session manager per account holder per company. If the installation directory was specified to be /usr/local then the session manager start up scripts will be found at /usr/local/STS/sessionmgr. The naming convention for the start up scripts is:

33

start\_<account holder name>.sh. Each account holder will have its own directory off of /usr/local/STS/sessionmgr.

With respect to the web server, once its configuration files have been modified as indicated above, the account holder access component will automatically be used once the web server is started. As web servers from different vendors require different start up procedures, it is assumed that this information is already known.

With respect to shutdown, of the system and particularly the web server, it is best to start with the secure transaction server as this is the first point of contact for the account holder's browser. Like the start up procedure for the web server, the shutdown procedure will differ for each different web server.

With respect to the session manager, it is recommended that shutdown of it be done from within the server side administration program. The browser should be pointed at the URL where the server site administration program is located and the administer button for the session manager that is wanted to be stopped should be clicked. A data dump on the session manager should be performed before stopping it to avoid loss of data contained within the manager to be stopped. This is executed by entering the complete pathname of the data dump file and clicking the data dump button. With respect to the transaction clearinghouse, the transaction clearinghouse daemons are shutdown using the kill command. The process identification numbers for each of the servers should be found by getting a list of all processes and searching for the process names of the start up procedures. Once the process identification numbers have been established, the command kill -9<pid>{<pid>} should be used.

With respect to the database server, it can be shutdown using the following steps:

---

```

login into isql as the system administrator
type "shutdown <backup database server name>"
type "go"
type "shutdown"
type "go"
hadji:>sql -Usa -P -SSTS
1> shutdown SYB_BACKUP
2> go
Backup Server: 3.48.1.1: The Backup Server will go down immediately.
Terminating sessions.
1> shutdown
2> go
Server SHUTDOWN by request.
The SQL Server is terminating this process.
00:97/05/14 14:52:40.23 server SQL Server shutdown by request.
00:97/05/14 14:52:40.24 kernel ushutdown: exiting DB-LIBRARY error:
Unexpected EOF from SQL Server.
hadji:>

```

---

It should be understood from the foregoing that a secure transaction system has been shown and described which enables a business to have total control over account holder access, transaction tracking and billing over an untrusted network such as the Internet world wide web. The system has many desirable attributes and features that enable it to provide such functionality. Moreover, it is extremely flexible in that it can operate to function with multiple servers and multiple transaction clearinghouses if desired. Moreover, two-factor authentication enables the system to frequently determine if a account holder is authentic and the system also functions to authenticate servers as well. A secure platform for businesses to securely provide transaction services to the world wide web in a way that assures revenue generation if that is a goal is a prominent feature of the system of the present invention.

34

While various embodiments of the present invention have been shown and described, it should be understood that other modifications, substitutions and alternatives are apparent to one of ordinary skill in the art. Such modifications, substitutions and alternatives can be made without departing from the spirit and scope of the invention, which should be determined from the appended claims.

Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

15 We claim:

1. A method for controlling access, by at least one authentication server, to protected computer resources provided via an Internet Protocol network, the method comprising:

receiving, at the at least one authentication server from at least one access server, identity data associated with at least one client computer device, the identity data forwarded to the at least one access server from the at least one client computer device with a request from the at least one client computer device for the protected computer resources;

authenticating, by the at least one authentication server, the identity data received from the at least one access server, the identity data being stored in the at least one authentication server;

authorizing, by the at least one authentication server, the at least one client computer device to receive at least a portion of the protected computer resources requested by the at least one client computer device, based on data associated with the requested protected computer resources stored in at least one database associated with the at least one authentication server; and

permitting access, by the at least one authentication server, to the at least the portion of the protected computer resources upon successfully authenticating the identity data and upon successfully authorizing the at least one client computer device.

2. The method of claim 1, wherein the Internet Protocol network comprises the Internet.

45 3. The method of claim 1, wherein the Internet Protocol network comprises TCP/IP.

4. The method of claim 1, wherein the Internet Protocol network comprises UDP/IP.

5. The method of claim 1, further comprising deriving the identity data from at least one internal hardware component of the at least one client computer device.

6. The method of claim 1, further comprising deriving the identity data from one of an external device and an external object connected to the at least one client computer device.

55 7. The method of claim 1, further comprising deriving the identity data from one of an external device and an external object inserted into a reader.

8. The method of claim 1, further comprising deriving the identity data from at least a portion of a plurality of hardware components associated with the at least one client computer device.

60 9. The method of claim 1, further comprising generating the identity data from at least one internal hardware component of the at least one client computer device.

65 10. The method of claim 1, further comprising generating the identity data from one of an external device and an external object inserted into a reader.

35

11. The method of claim 1, further comprising generating the identity data from at least a portion of a plurality of hardware components associated with the at least one client computer device,

12. The method of claim 1, wherein the identity data comprises a digital certificate associated with the at least one client computer device.

13. The method of claim 1, wherein the identity data associated with the at least one client computer device is encrypted.

14. The method of claim 13, wherein the identity data associated with the at least one client computer device is encrypted using at least one asymmetric key.

15. The method of claim 13, wherein the identity data associated with the at least one client computer device is encrypted using at least one symmetric key.

16. The method of claim 1, wherein the identity data associated with the at least one client computer device contains at least one hash value.

17. The method of claim 1, wherein the client computer device authenticates the access server.

18. The method of claim 1, wherein the receiving of the identity data associated with the at least one client computer device includes the receiving of the identity data associated with the at least one client computer device and at least one of a username and a password.

19. The method of claim 1, further comprising encrypting at least a portion of the identity data.

20. The method of claim 1, wherein the identity data associated with the at least one client computer device is known in advance.

21. The method of claim 1, wherein the identity data associated with the at least one client computer device is unique.

22. The method of claim 21, wherein the identity data associated with the at least one client computer device is unique to the at least one client computer device.

23. The method of claim 21, wherein the identity data associated with the at least one client computer device is unique to a group of client computer devices comprising the at least one client computer device.

24. The method of claim 1, wherein the identity data being stored in the at least one authentication server is stored in at least one database associated with the at least one authentication server.

25. The method of claim 1, further comprising storing the at least the portion of the protected computer resources on at least one server computer associated with the at least one access server.

26. The method of claim 1, further comprising providing, by at least one server associated with the at least one access server, the at least the portion of the requested protected computer resources to the at least one client computer device upon the at least one authentication server permitting access to the at least the portion of the protected computer resources.

27. The method of claim 1, further comprising storing the at least the portion of the protected computer resources in at least one of a plurality of server computers associated with the at least one access server.

28. The method of claim 1, further comprising storing the at least the portion of the protected computer resources in the at least one access server.

29. The method of claim 1, further comprising providing, by at least one of a plurality of multiple servers associated with the at least one access server, the at least the portion of the requested protected computer resources to the at least one

36

client computer device upon the at least one authentication server permitting access to the at least the portion of protected computer resources.

30. The method of claim 1, further comprising encrypting at least a portion of the protected computer resources.

31. The method of claim 1, further comprising locating the at least one authentication server on a computer separate from the at least one access server.

32. The method of claim 1, further comprising locating the at least one authentication server on the same computer as the at least one access server.

33. The method of claim 1, wherein at least one of the functions of the at least one authentication server are performed by another server associated with the at least one authentication server.

34. The method of claim 1, wherein authenticating, by the at least one authentication server, includes the at least one authentication server authenticating multiple client computer devices.

35. The method of claim 1, wherein authenticating, by the at least one authentication server, includes the at least one authentication server authenticating multiple access servers.

36. The method of claim 1, wherein authenticating, by the at least one authentication server, is performed by one of a plurality of servers associated with the at least one authentication server.

37. The method of claim 1, wherein authorizing, by the at least one authentication server, is performed by one of a plurality of servers associated with the at least one authentication server.

38. The method of claim 1, wherein permitting, by the at least one authentication server, is performed by one of a plurality of servers associated with the at least one authentication server.

39. The method of claim 1, further comprising assigning one of a plurality of authorization levels to the at least a portion of the protected computer resources, assigning a particular authorization level to the identity data associated with the at least one client computer device, and only permitting access to particular protected computer resources by the at least one client computer device permitted by the particular authorization level.

40. The method of claim 1, wherein the storing of the identity data includes storing identity data associated with the at least one access server in the at least one authentication server.

41. The method of claim 40, further comprising forwarding the identity data associated with the at least one access server to the at least one authentication server.

42. The method of claim 41, further comprising authenticating the identity data associated with the at least one access server by the at least one authentication server responsive to the at least one client computer device making the request for the at least a portion of the protected computer resources.

43. The method of claim 42, further comprising permitting access to the requested at least a portion of the protected computer resources, wherein such permitting access includes permitting access by the at least one authentication server to the at least a portion of the protected computer resources responsive to successfully authenticating the at least one access server and the at least one client computer device making the request.

44. The method of claim 1, further comprising providing, by the at least one access server, the at least the portion of the requested protected computer resources to the at least one client computer device upon the at least one authentication

server permitting access to the at least the portion of the protected computer resources.

**45.** The method of claim 1, further comprising selectively requiring the client computer device to forward its identity data to the at least one access server.

**46.** The method of claim 1, further comprising selectively prompting the at least one client computer device to provide its identity data and at least one of a username and a password.

**47.** The method of claim 1, further comprising selectively querying the at least one client computer device to generate the identity data associated with the at least one client computer device.

**48.** The method of claim 1, further comprising changing, by the at least one access server, the identity data associated with the at least one client computer device, and forwarding the changed identity data to the at least one authentication server.

**49.** A method for controlling access, by at least one authentication server, to protected computer resources provided via an Internet Protocol network, the method comprising:

receiving, at the at least one authentication server from at least one access server, identity data of the at least one access server and identity data associated with at least one client computer device, the identity data associated with the at least one client computer device forwarded to the at least one access server from the at least one client computer device with a request from the at least one client computer device for the protected computer resources;

authenticating, by the at least one authentication server, the identity data of the at least one access server and the identity data associated with the at least one client computer device received from the at least one access server, the identity data of the at least one access server and the identity data associated with the at least one client computer device being stored in the at least one authentication server;

authorizing, by the at least one authentication server, the at least one client computer device to receive at least a portion of the protected computer resources requested by the at least one client computer device, based on data associated with the requested protected computer resources stored in at least one database associated with the at least one authentication server; and

permitting access, by the at least one authentication server, to the at least the portion of the protected computer resources upon successfully authenticating the identity data of the at least one access server and the identity data of the at least one client computer device and upon successfully authorizing the at least one client computer device.

**50.** The method of claim 49, wherein the Internet Protocol network comprises the Internet.

**51.** The method of claim 49, wherein the Internet Protocol network comprises TCP/IP.

**52.** The method of claim 49, wherein the Internet Protocol network comprises UDP/IP.

**53.** The method of claim 49, further comprising deriving the identity data associated with the at least one client computer device from at least one internal hardware component of the at least one client computer device.

**54.** The method of claim 49, further comprising deriving the identity data associated with the at least one client computer device from one of an external device and an external object connected to the at least one client computer device.

**55.** The method of claim 49, further comprising deriving the identity data associated with the at least one client computer device from one of an external device and an external object inserted into a reader.

**56.** The method of claim 49, further comprising deriving the identity data associated with the at least one client computer device from at least a portion of a plurality of hardware components associated with the at least one client computer device.

**57.** The method of claim 49, further comprising generating the identity data associated with the at least one client computer device from at least one internal hardware component of the at least one client computer device.

**58.** The method of claim 49, further comprising generating the identity data associated with the at least one client computer device from one of an external device and an external object inserted into a reader.

**59.** The method of claim 49, further comprising generating the identity data associated with the at least one client computer device from at least a portion of a plurality of hardware components associated with the at least one client computer device.

**60.** The method of claim 49, wherein the identity data associated with the at least one client computer device comprises a digital certificate associated with the at least one client computer device.

**61.** The method of claim 49, wherein the identity data associated with the at least one client computer device is encrypted.

**62.** The method of claim 61, wherein the identity data associated with the at least one client computer device is encrypted using at least one asymmetric key.

**63.** The method of claim 61, wherein the identity data associated with the at least one client computer device encrypted using at least one symmetric key.

**64.** The method of claim 49, wherein the identity data associated with the at least one client computer device contains at least one hash value.

**65.** The method of claim 49, wherein the client computer device authenticates the access server.

**66.** The method of claim 49, wherein the receiving of the identity data associated with the at least one client computer device includes the receiving of the identity data associated with the at least one client computer device and at least one of a username and a password.

**67.** The method of claim 49, further comprising encrypting at least a portion of the identity data associated with the at least one client computer device.

**68.** The method of claim 49, wherein the identity data associated with the at least one client computer device is known in advance.

**69.** The method of claim 49, wherein the identity data associated with the at least one client computer device is unique.

**70.** The method of claim 69, wherein the identity data associated with the at least one client computer device is unique to the at least one client computer device.

**71.** The method of claim 69, wherein the identity data associated with the at least one client computer device is unique to a group of client computer devices comprising the at least one client computer device.

**72.** The method of claim 49, wherein the identity data associated with the at least one client computer device being stored in the at least one authentication server is stored in at least one database associated with the at least one authentication server.

**73.** The method of claim 49, further comprising storing the at least the portion of the protected computer resources on at least one server computer associated with the at least one access server.

**74.** The method of claim 49, further comprising providing, by at least one server associated with the at least one access server, the at least the portion of the requested protected computer resources to the at least one client computer device upon the at least one authentication server permitting access to the at least the portion of the protected computer resources.

**75.** The method of claim 49, further comprising storing the at least the portion of the protected computer resources in at least one of a plurality of server computers associated with the at least one access server.

**76.** The method of claim 49, further comprising storing the at least the portion of the protected computer resources in the at least one access server.

**77.** The method of claim 49, further comprising providing, by at least one of a plurality of multiple servers associated with the at least one access server, the at least the portion of the requested protected computer resources to the at least one client computer device upon the at least one authentication server permitting access to the at least the portion of protected computer resources.

**78.** The method of claim 49, further comprising encrypting at least a portion of the protected computer resources.

**79.** The method of claim 49, further comprising locating the at least one authentication server on a computer separate from the at least one access server.

**80.** The method of claim 49, further comprising locating the at least one authentication server on the same computer as the at least one access server.

**81.** The method of claim 49, wherein at least one of the functions of the at least one authentication server are performed by another server associated with the at least one authentication server.

**82.** The method of claim 49, wherein authenticating, by the at least one authentication server, includes the at least one authentication server authenticating multiple client computer devices.

**83.** The method of claim 49, wherein authenticating, by the at least one authentication server, includes the at least one authentication server authenticating multiple access servers.

**84.** The method of claim 49, wherein authenticating, by the at least one authentication server, is performed by one of a plurality of servers associated with the at least one authentication server.

**85.** The method of claim 49, wherein authorizing, by the at least one authentication server, is performed by one of a plurality of servers associated with the at least one authentication server.

**86.** The method of claim 49, wherein permitting, by the at least one authentication server, is performed by one of a plurality of servers associated with the at least one authentication server.

**87.** The method of claim 49, further comprising assigning one of a plurality of authorization levels to the at least a portion of the protected computer resources, assigning a particular authorization level to the identity data associated with the at least one client computer device, and only permitting access to particular protected computer resources by the at least one client computer device permitted by the particular authorization level.

**88.** The method of claim 49, further comprising providing, by the at least one access server, the at least the portion of the requested protected computer resources to the at least one client computer device upon the at least one authentication server permitting access to the at least the portion of the protected computer resources.

**89.** The method of claim 49, further comprising selectively requiring the client computer device to forward its identity data associated with the at least one client computer device to the at least one access server.

**90.** The method of claim 49, further comprising selectively prompting the at least one client computer device to provide its identity data and at least one of a username and a password.

**91.** The method of claim 49, further comprising selectively querying the at least one client computer device to generate the identity data associated with the at least one client computer device.

**92.** The method of claim 49, further comprising changing, by the at least one access server, the identity data associated with the at least one client computer device, and forwarding the changed identity data to the at least one authentication server.

\* \* \* \* \*

# The United States of America



## The Director of the United States Patent and Trademark Office

*Has received an application for a patent for a new and useful invention. The title and description of the invention are enclosed. The requirements of law have been complied with, and it has been determined that a patent on the invention shall be granted under the law.*

*Therefore, this*

## United States Patent

*Grants to the person(s) having title to this patent the right to exclude others from making, using, offering for sale, or selling the invention throughout the United States of America or importing the invention into the United States of America for the term set forth below, subject to the payment of maintenance fees as provided by law.*

*If this application was filed prior to June 8, 1995, the term of this patent is the longer of seventeen years from the date of grant of this patent or twenty years from the earliest effective U.S. filing date of the application, subject to any statutory extension.*

*If this application was filed on or after June 8, 1995, the term of this patent is twenty years from the U.S. filing date, subject to any statutory extension. If the application contains a specific reference to an earlier filed application or applications under 35 U.S.C. 120, 121 or 365(c), the term of the patent is twenty years from the date on which the earliest application was filed, subject to any statutory extensions.*

A handwritten signature in black ink, appearing to read "James M. Rogan".

*Director of the United States Patent and Trademark Office*

Trial Exhibit

**TX 2**

Case No. 8:12-CV-123-LES-TDT

TX0002-0001

## **NOTICE**

*If the application for this patent was filed on or after December 12, 1980, maintenance fees are due three years and six months, seven years and six months, and eleven years and six months after the date of this grant, or within a grace period of six months thereafter upon payment of a surcharge as provided by law. The amount, number of timing of the maintenance fees required may be changed by law or regulation. Unless payment of the applicable maintenance fee is received in the United States Patent and Trademark Office on or before the date the fee is due or within a grace period of six months thereafter, the patent will expire as of the end of such grace period.*



US008387155B2

(12) **United States Patent**  
Gregg et al.

(10) **Patent No.:** US 8,387,155 B2  
(45) **Date of Patent:** \*Feb. 26, 2013

(54) **SYSTEM FOR MANAGING ACCESS TO PROTECTED COMPUTER RESOURCES**

(75) Inventors: **Richard L. Gregg**, Elkhorn, NE (US);  
**Sandeep Giri**, Omaha, NE (US);  
**Timothy C. Goeke**, Elkhorn, NE (US)

(73) Assignee: **Prism Technologies LLC**, Omaha, NE (US)

(\*) Notice: Subject to any disclaimer, the term of this patent is extended or adjusted under 35 U.S.C. 154(b) by 0 days.

This patent is subject to a terminal disclaimer.

(21) Appl. No.: **12/944,473**

(22) Filed: **Nov. 11, 2010**

(65) **Prior Publication Data**

US 2011/0061097 A1 Mar. 10, 2011

**Related U.S. Application Data**

(63) Continuation of application No. 11/978,919, filed on Oct. 30, 2007, now Pat. No. 8,127,345, which is a continuation of application No. 10/230,638, filed on Aug. 29, 2002, now Pat. No. 7,290,288, which is a continuation-in-part of application No. 08/872,710, filed on Jun. 11, 1997, now Pat. No. 6,516,416.

(51) **Int. Cl.**

**G06F 21/20** (2006.01)

(52) **U.S. Cl.** ..... **726/29; 726/7**

(58) **Field of Classification Search** ..... **726/7, 29**  
See application file for complete search history.

(56) **References Cited**

## U.S. PATENT DOCUMENTS

4,446,519 A 5/1984 Thomas  
(Continued)

## FOREIGN PATENT DOCUMENTS

EP 0 636 963 A2 2/1995  
EP 0 762 261 A2 9/1996  
(Continued)

## OTHER PUBLICATIONS

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Verified Complaint Under Section 337 of the Tariff Act of 1930, As Amended; 26 pages; Exhibit 2, 11 pages; Exhibit 3, 31 pages; Exhibit 4, 31 pages; Exhibit 5, 1 page; Exhibit 6, 4 pages; Exhibit 7, 31 pages; Exhibit 8, 2 pages; Exhibit 9, 92 pages; Exhibit 10, 4 pages; Exhibit 11, 92 pages; Exhibit 12, 56 pages; Exhibit 13, 17 pages; Exhibit 26, 2 pages; Exhibit 29, 10 pages; Exhibit 30, 1 page; Exhibit 31, 1 page; Exhibit 32, 4 pages; Exhibit 34, 19 pages; Exhibit 35, 3 pages; Exhibit 36, 1 page; Exhibit 37, 169 pages; Letter Submiting Verified Complaint to the International Trade Comission; 2 pages; Letter Requesting Confidential Treatment of Exhibits; 2 pages; Dec. 2, 2009.

(Continued)

*Primary Examiner* — Kambiz Zand

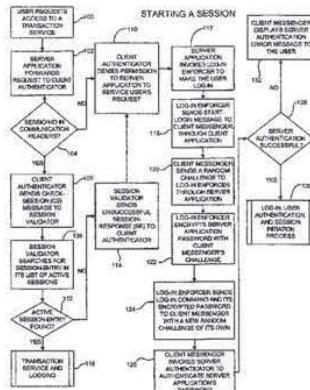
*Assistant Examiner* — Aubrey Wyszynski

(74) *Attorney, Agent, or Firm* — Martin & Ferraro, LLP

(57) **ABSTRACT**

A system for controlling access to protected computer resources provided via a network utilizing at least one Internet Protocol. The system includes at least one authentication server and at least one access server. The at least one authentication server is adapted to authenticate identity data associated with at least one client computer device, is adapted to authorize the at least one client computer device to receive at least a portion of protected computer resources, and is adapted to permit access to the at least a portion of the protected computer resources. The at least one access server is adapted to receive the identity data associated with the at least one client computer device and forward the identity data associated with the at least one client computer device to the at least one authentication server.

**97 Claims, 27 Drawing Sheets**



TX0002-0003

# US 8,387,155 B2

Page 2

## U.S. PATENT DOCUMENTS

4,471,163 A	9/1984	Donald et al.	5,677,955 A	10/1997	Doggett et al.
4,652,990 A	3/1987	Pailen et al.	5,687,235 A	11/1997	Renner et al.
4,658,093 A	4/1987	Hellman	5,696,824 A	12/1997	Perlman et al.
4,685,055 A	8/1987	Thomas	5,699,431 A	12/1997	Walsh
4,691,355 A	9/1987	Wirstrom et al.	5,706,427 A	1/1998	Van Oerschot et al.
4,694,492 A	9/1987	Wirstrom et al.	5,708,780 A	1/1998	Tabuki
4,748,561 A	5/1988	Brown	5,710,884 A	1/1998	Levergood et al.
4,796,220 A	1/1989	Wolfe	5,715,314 A	2/1998	Dedrick
4,864,494 A	9/1989	Kobus, Jr.	5,717,756 A *	2/1998	Payne et al.
4,866,769 A	9/1989	Karp	5,717,757 A	2/1998	Coleman ..... 713/155
4,885,789 A	12/1989	Burger et al.	5,717,758 A	2/1998	Micali
4,907,268 A	3/1990	Bosen et al.	5,721,781 A	2/1998	Micall
4,916,738 A	4/1990	Chandra et al.	5,724,424 A	3/1998	Deo et al.
4,932,054 A	6/1990	Chou et al.	5,737,416 A	4/1998	Gifford
4,935,962 A	6/1990	Austin	5,740,361 A	4/1998	Cooper et al.
4,962,449 A	10/1990	Schlesinger	5,754,864 A	4/1998	Brown
4,977,594 A	12/1990	Shear	5,757,907 A	5/1998	Hill
4,999,806 A	3/1991	Chernow et al.	5,758,069 A	5/1998	Cooper et al.
5,032,979 A	7/1991	Hecht et al.	5,761,306 A	6/1998	Olsen
5,048,085 A	9/1991	Abraham et al.	5,761,309 A	6/1998	Lewis
5,060,263 A	10/1991	Bosen et al.	5,761,649 A	6/1998	Ohashi et al.
5,081,676 A	1/1992	Chou et al.	5,765,152 A	6/1998	Hill
5,103,476 A	4/1992	Waite et al.	5,774,552 A	6/1998	Erickson
5,138,712 A	8/1992	Corbin	5,778,071 A	7/1998	Grimmer
5,182,770 A	1/1993	Medveczky et al.	5,778,072 A	7/1998	Caputo et al.
5,199,066 A	3/1993	Logan	5,781,723 A	7/1998	Samar
5,204,961 A	4/1993	Barlow	5,784,464 A	7/1998	Yee et al.
5,222,133 A	6/1993	Chou et al.	5,790,677 A	7/1998	Akiyama et al.
5,222,134 A	6/1993	Waite et al.	5,793,868 A	8/1998	Micali
5,229,764 A *	7/1993	Matchett et al. .... 340/5.52	5,809,144 A	9/1998	Sirbu et al.
5,235,642 A	8/1993	Wobber et al.	5,809,145 A	9/1998	Slik et al.
5,237,614 A	8/1993	Weiss	5,815,665 A	9/1998	Teper et al.
5,247,575 A	9/1993	Sprague et al.	5,826,011 A	10/1998	Chou et al.
5,260,999 A	11/1993	Wyman	5,841,970 A *	11/1998	Tabuki ..... 726/2
5,291,598 A	3/1994	Grundy	5,864,620 A	1/1999	Pettitt
5,315,657 A	5/1994	Abadi et al.	5,878,142 A	3/1999	Caputo et al.
5,337,357 A	8/1994	Chou et al.	5,889,958 A	3/1999	Willens
5,347,580 A	9/1994	Molva et al.	5,892,900 A	4/1999	Ginter et al.
5,349,643 A	9/1994	Cox et al.	5,903,652 A	5/1999	Mital
5,357,573 A	10/1994	Walters	5,910,987 A	6/1999	Ginter et al.
5,371,794 A	12/1994	Diffee et al.	5,922,074 A	7/1999	Richard et al.
5,373,561 A	12/1994	Haber et al.	5,926,624 A	7/1999	Katz et al.
5,375,240 A	12/1994	Grundy	5,930,804 A	7/1999	Yu et al.
5,379,343 A	1/1995	Grube et al.	5,938,350 A	8/1999	Colonel
5,414,844 A	5/1995	Wang	5,940,504 A	8/1999	Griswold
5,416,842 A	5/1995	Aziz	5,943,423 A	8/1999	Muflic
5,428,745 A	6/1995	De Bruijn et al.	5,969,316 A	10/1999	Greer et al.
5,442,708 A	8/1995	Adams, Jr. et al.	5,982,898 A	11/1999	Hsu et al.
5,444,782 A	8/1995	Adams et al.	5,983,350 A	11/1999	Minear et al.
5,455,953 A	10/1995	Russell	5,987,232 A	11/1999	Tabuki
5,483,596 A	1/1996	Rosenow et al.	5,999,711 A	12/1999	Misra et al.
5,485,409 A	1/1996	Gupta et al.	6,003,135 A	12/1999	Bialick et al.
5,490,216 A	2/1996	Richardson, III	6,005,939 A	12/1999	Fortenberry et al.
5,491,804 A	2/1996	Heath et al.	6,006,332 A	12/1999	Rabne et al.
5,497,421 A	3/1996	Kaufman et al.	6,021,202 A	2/2000	Anderson et al.
5,499,297 A	3/1996	Boebert	6,035,402 A	3/2000	Vaeth et al.
5,502,766 A	3/1996	Boebert et al.	6,041,357 A	3/2000	Kunzelman et al.
5,502,831 A	3/1996	Grube et al.	6,041,411 A	3/2000	Wyatt
5,509,070 A	4/1996	Schull	6,044,471 A	3/2000	Colvin
5,511,122 A	4/1996	Atkinson	6,047,376 A	4/2000	Hosoe
5,535,276 A	7/1996	Ganesan	6,052,785 A	4/2000	Lin et al.
5,539,828 A	7/1996	Davis	6,070,243 A	5/2000	See et al.
5,546,463 A	8/1996	Caputo et al.	6,075,860 A	6/2000	Ketcham
5,572,673 A	11/1996	Shurts	6,088,451 A	7/2000	He et al.
5,588,059 A	12/1996	Chandos et al.	6,108,420 A	8/2000	Larose et al.
5,590,197 A	12/1996	Chen et al.	6,173,403 B1	1/2001	DeMont
5,590,199 A	12/1996	Krajewski, Jr. et al.	6,185,587 B1	2/2001	Bernardo et al.
5,592,553 A	1/1997	Guski et al.	6,212,634 B1	4/2001	Geer, Jr. et al.
5,604,804 A	2/1997	Micali	6,219,790 B1	4/2001	Lloyd et al.
5,606,615 A	2/1997	Laponte et al.	6,223,984 B1	5/2001	Renner et al.
5,623,637 A	4/1997	Jones et al.	6,226,744 B1	5/2001	Murphy et al.
5,629,980 A	5/1997	Stefik et al.	6,247,011 B1	6/2001	Jecha et al.
5,634,012 A	5/1997	Stefik et al.	6,249,873 B1	6/2001	Richard et al.
5,657,390 A	8/1997	Elgamal et al.	6,256,737 B1	7/2001	Bianco et al.
5,659,616 A	8/1997	Sudia	6,377,994 B1 *	4/2002	Ault et al. ..... 709/229
5,666,411 A	9/1997	McCarty	6,510,236 B1	1/2003	Crane et al.
5,666,416 A	9/1997	Micali	6,516,416 B2	2/2003	Gregg et al.
5,677,953 A	10/1997	Dolphin	6,553,492 B1	4/2003	Hosoe

TX0002-0004

6,615,258 B1	9/2003	Barry et al.
7,039,021 B1	5/2006	Kokudo
7,117,376 B2	10/2006	Gravrock
7,231,661 B1	6/2007	Villavicencio et al.
7,233,997 B1	6/2007	Leveridge et al.
7,275,260 B2	9/2007	de Jong et al.
7,290,288 B2 *	10/2007	Gregg et al. .... 726/28
7,502,726 B2	3/2009	Panasyuk et al.
7,920,706 B2	4/2011	Asokan et al.
2004/0024764 A1	2/2004	Hsu et al.

## FOREIGN PATENT DOCUMENTS

EP	0 935 221 A2	8/1999
JP	9-81518 A	9/1995
JP	9-81519 A	9/1995
JP	10-285156 A	10/1998
WO	WO 94/26044 A2	11/1994
WO	WO 96/07256 A1	3/1996
WO	WO 00/46681 A1	8/2000

## OTHER PUBLICATIONS

In re Certain Authentication Systems, Including Software and Handheld Electronic Devices; Docket No. 2699; Public Version of Confidential Submissions; 3 pages; Exhibit 19, 3 pages; Exhibit 20, 4 pages; Exhibit 39, 2 pages; Dec. 18, 2009.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Response of Respondents Research in Motion Limited and Research in Motion Corporation to the Verified Complaint and Notice of Investigation; 27 pages; Exhibit A, 21 pages; Exhibit A-1, 421 pages; Exhibit A-2, 145 pages; Exhibit B, 37 pages; Exhibit C, 47 pages; Exhibit D, 35 pages; Exhibit E, 49 pages; Exhibit F, 37 pages; Exhibit G, 34 pages; Exhibit H, 28 pages; Jan. 20, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Complainant Prism Technologies' Supplemental Response to Research in Motion Corporation's Interrogatory No. 4; 6 pages; Feb. 26, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Complainant Prism Technologies' Amended Response to Research in Motion Corporation's Interrogatory No. 4; 8 pages; Mar. 11, 2010. In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Complainant Prism Technologies' Amended Responses to Research in Motion Limited's Interrogatories Nos. 13 and 16; 9 pages; Mar. 11, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Complainant Prism Technologies' Supplemental Response to Respondent Research in Motion Limited's Interrogatories Nos. 13-19; 87 pages; Mar. 24, 2010.

In the Matter of: Certain Authentication Systems; Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Respondent Research in Motion Corporation's Supplemental Response to Prism's Interrogatory No. 25; 9 pages; Mar. 26, 2010. In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Respondent Research in Motion Limited's Supplemental Response to Prism's Interrogatory No. 25; 9 pages; Mar. 26, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are invalid; 4 pages; Mar. 29, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Memorandum in Support of Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; Redacted Version; 10 pages; Mar. 29, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Statement of Material Facts for Which There is No Genuine Issue Accompanying Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; Redacted Version; 7 pages; Mar. 29, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Declaration of Christopher R. Liro in Support of Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; 3 pages; Exhibit C, 98 pages; Exhibit E, 10 pages; Exhibit F, 6 pages; Mar. 29, 2010.

In the Matter of Certain Authentication Systems, including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Declaration of Charles J. Hawkins: (1) in Support of Motion of Complainant Prism Technologies LLC for 45-Day Stay of the Proceedings and Shortened Response Period Hereto; and (2) in Opposition to Motion of Respondents Research in Motion Limited and Research in Motion Corporation for Summary Determination that the Asserted Claims of U.S. Patent No. 7,290,288 are Invalid; 6 pages; Exhibit A, 2 pages; Exhibit B, 3 pages; Exhibit C, 2 pages; Exhibit E, 2 pages; Exhibit F, 7 pages; Exhibit G, 13 pages; Exhibit H, 16 pages; Exhibit I, 5 pages; Exhibit J, 10 pages; Exhibit K, 6 pages; Exhibit L, 17 pages; Exhibit M, 62 pages; Exhibit N, 6 pages; Exhibit R, 4 pages; Exhibit T, 53 pages; Apr. 12, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent 7,290,288, Motion Docket No. 697-006; 30 pages; Apr. 12, 2010.

In the Matter of Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Prism Technologies, LLC's Response to RIM's Statement of Material Facts for Which There is No Genuine Issue; 17 pages; Apr. 12, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Motion of Respondents Research in Motion Limited and Research in Motion Corporation to File a Reply to Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent No. 7,290,288; 4 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Memorandum in Support of Motion of Respondents Research in Motion Limited and Research in Motion Corporation to File a Reply to Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent No. 7,290,288; 3 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; RIM's Reply to Prism's Response to RIM's Motion for Summary Determination of Invalidity of the Asserted Claims of U.S. Patent No. 7,290,288; Redacted Version; 11 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; RIM's Response to Prism's Prism Technologies, LLC's Statement of Material Facts; 13 pages; Apr. 19, 2010.

In the Matter of: Certain Authentication Systems, Including Software and Handheld Electronic Devices; Investigation No. 337-TA-697; Respondents' Research in Motion Limited and Research in Motion Corporation Opposition to Complainant Prism Technologies LLC's Motion for 45-Day Stay of the Proceedings (Motion No. 697-012); Redacted Version; 18 pages; Apr. 22, 2010.

*Prism Technologies LLC, v. Verisign, Inc., et al.; Civil Action No. 05-214 JMF; Defendants' Second Supplemental Joint 35 U.S.C. § 282 Notice; Mar. 12, 2007; 7 pages; Exhibit A, pp. 1-80.*

*Prism Technologies LLC, v. Verisign, Inc., et al.; Civil Action No. 05-214-JMF; Plaintiffs First Amended Complaint for Patent Infringement and Demand for Jury Trial, Jun. 22, 2005; 7 pages.*

*Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. CA 05-00214 JJF; Plaintiff's Second Amended Complaint for Patent Infringement and Demand for Jury Trial; Aug. 11, 2006; 7 pages. Plaintiff's Complaint for Patent Infringement and Demand for Jury Trial; *Prism Technologies, LLC v. Verisign, Inc., et al.*; dated Apr. 11, 2005; pp. 1-6.

Defendants' Joint Invalidity Contentions and Joint Supplemental Answer and Objections to Plaintiff's Interrogatory No. 4; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 05-214-JJF; Sep. 5, 2006; 118 pages.

Defendants' Joint Supplemental Invalidity Contentions in Response to Plaintiff's Interrogatory No. 4; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 1:05-cv-00214-JJF; dated Mar. 12, 2007; 269 pages.

Defendants' Opening Claim Construction Brief and Appendix with Exhibits; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 05-214-JJF; dated Sep. 22, 2006; 540 pages.

Defendants' Responsive Claim Construction Brief with Exhibits (Public Version); *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 05-214-JJF; dated Oct. 17, 2006; 85 pages.

Plaintiff Prism Technologies LLC's Claim Construction Answering Brief with Exhibits; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 05-214-JJF; dated Oct. 13, 2006; 74 pages.

Plaintiff Prism Technologies LLC's Opening Claim Construction Brief and Appendix with Exhibits; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 05-214-JJF; dated Sep. 22, 2006; 145 pages.

Memorandum Opinion; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 1:05-cv-00214-JJF; Document 448; filed Apr. 2, 2007; 41 pages.

Order; *Prism Technologies LLC v. Verisign, Inc., et al.*; Civil Action No. 1:05-cv-00214-JJF; Document 449; filed Apr. 2, 2007; 7 pages.

*Prism Technologies LLC, v. Verisign, Inc., et al.*; Civil Action No. 05-214 JJF; Plaintiff Prism Technologies LLC's Objections and Responses to Defendant Nete格ity, Inc.'s First Set of Interrogatories (Nos. 1-5); Oct. 24, 2005; 18 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd., et al.*; Case No. 8:08-CV-537; Complaint; Dec. 29, 2008; pp. 1-5.

*Prism Technologies LLC, v. Research in Motion, Ltd.*; Case No. 8:08-cv-00537-LES-TDT; Joint Claim Construction Statement; Document No. 72; Oct. 16, 2009; pp. 1-6.

*Prism Technologies LLC, v. Research in Motion, Ltd., et al.*; Case No. 8:08-cv-00537-LES-TDT; Plaintiff's Disclosure of Asserted Claims and Preliminary Infringement Contentions Regarding Defendant Microsoft Corporation; Jun. 26, 2009; 4 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd., et al.*; Case No. 8:08-cv-00537-LES-TDT; Plaintiff's Disclosure of Asserted Claims and Preliminary Infringement Contentions Regarding Defendant Research in Motion, Ltd.; Jun. 26, 2009; 4 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd., et al.*; Case No. 8:08-cv-00537-LES-TDT; Defendant Research in Motion, Ltd.'s Amended Invalidity Contentions; Sep. 18, 2009; 7 pages; Akiyama Chart, 65 pages; Yu Chart, 72 pages; Tabuki Chart, 52 pages; Teper Chart, 54 pages; Grawrock Chart, 39 pages; Crane Chart, 37 pages; Murphy Chart, 38 pages; He Chart, 45 pages; Ketcham Chart, 74 pages; Krajewski Chart, 127 pages; DCE Chart (redacted), 192 pages; SiteMinder Chart, 61 pages; Handbook of Applied Cryptography Chart, 124 pages; Kerberos V5 Chart, 46 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd.*; Case No. 8:08-cv-00537-LES-TDT; Plaintiff's Amended Disclosure of Asserted Claims and Preliminary Infringement Contentions; Feb. 5, 2010; 6 pages; Exhibit A, cover page and pp. 1-134.

Microsoft Corporation's Preliminary Invalidity Contentions; *Prism Technologies, LLC v. Research in Motion, Ltd., and Microsoft Corporation*; Case No. 8:08-CV-537; dated Jul. 24, 2009; pp. 1-77.

Defendant Research in Motion, Ltd.'s Preliminary Invalidity Contentions; *Prism Technologies, LLC v. Research in Motion, Ltd., and Microsoft Corporation*; Case No. 8:08-cv-00537-LES-TDT; dated Jul. 24, 2009; 249 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd.*; Case No. 8:08-cv-00537-LES-TDT; Second Supplemental Responses to Research in Motion, Ltd.'s Interrogatories Nos. 5, 6 and 8; Feb. 16, 2010; 12 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd.*; Case No. 8:08-cv-00537-LES-TDT; Defendant Research in Motion, Ltd.'s Second Amended Invalidity Contentions; Apr. 23, 2010; 10 pages; Akiyama Chart, 65 pages; Crane Chart, 37 pages; DTN Cookie-Authentication System, 40 pages; Encrypted File Transfer System Without Key Management-Secure-flip Chart, 30 pages; Gifford Chart, 46 pages; Grawrock Chart, 39 pages; Handbook of Applied Cryptography, 124 pages; He Chart, 45 pages; Kerberos V5 Chart, 39 pages; Krajewski Chart, 127 pages; Murphy Chart, 38 pages; NeTegrity SiteMinder Product Chart, 175 pages; Rainbow Sentinel SuperPro Chart, 69 pages; Secure Access Markup Language/SAML V 1.0 Chart, 114 pages; SET Secure Electronic Transaction Specification Version 1.0 Chart, 53 pages; Study of an Authentication Protocol in a Distributed System Environment Chart, 40 pages; Tabuki Chart, 52 pages; Teper Chart, 54 pages; Ketcham Chart, 74 pages; Yu Chart, 72 pages; Weiss Chart, 46 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd.*; Case No. 8:08-cv-00537; Second Amended Answer and Counterclaim of Defendant Research in Motion, Ltd.; Apr. 29, 2010; 28 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd.*; No. 8:08-CV-537; Research in Motion, Ltd.'s Response to Plaintiff Prism Technologies LLC's Opening Claim Construction Brief; Document 94; Dec. 4, 2009; 50 pages.

*Prism Technologies LLC, v. Research in Motion, Ltd.*; No. 8:08-CV-537; Index of Evidence in Support of Research in Motion, Ltd.'s Response to Plaintiff Prism Technologies LLC's Opening Claim Construction Brief; Document 95; Dec. 4, 2009; 4 pages; Exhibit A, 4 pages; Exhibit C, 4 pages; Exhibit D, 3 pages; Exhibit E, 68 pages; Exhibit F, 24 pages; Exhibit G, 27 pages; Exhibit L, 42 pages; Exhibit M, 7 pages; Exhibit N, 3 pages.

*Prism Technologies, LLC, v. Research in Motion, Ltd.*; 8:08CV537; Order; Document No. 132; Feb. 22, 2010; 1 page.

*Prism Technologies, LLC, v. Research in Motion, Ltd.*; 8:08-CV-537; Plaintiff Prism Technologies' Reply Brief on Claim Construction; Document No. 154; Mar. 22, 2010; 34 pages.

*Prism Technologies, LLC, v. Research in Motion, Ltd.*; 8:08-CV-537; Index of Evidence in Support of Plaintiff Prism Technologies' Reply Brief on Claim Construction; Document No. 155; Mar. 22, 2010; 3 pages; Exhibit D, 17 pages; Exhibit E, 3 pages; Exhibit F, 11 pages; Exhibit G, 69 pages; Exhibit H, 2 pages.

Defendant Symantec Corp.'s Answer, Affirmative Defenses, and Counterclaims; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 107; filed Aug. 23, 2010; 13 pages.

Defendant Autodesk, Inc.'s Answer and Counterclaims; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 108; filed Aug. 23, 2010; 12 pages.

Defendant Sage Software, Inc.'s Answer to Prism's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 113; filed Sep. 1, 2010; 11 pages.

Defendant Nuance, Inc.'s Answer and Counterclaims; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 119; filed Sep. 7, 2010; 34 pages.

Defendant National Instruments Corp.'s Answer and Counterclaims to Plaintiff's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 120; filed Sep. 7, 2010; 12 pages.

Answer and Counterclaims of Defendant Trend Micro Incorporated to Plaintiff Prism Technologies, LLC's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 121; filed Sep. 7, 2010; 14 pages.

Defendant Adobe Systems Inc.'s Answer and Counterclaims to Plaintiff's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 123; filed Sep. 7, 2010; 13 pages.

Defendant Quark, Inc.'s Answer and Counterclaims to Prism Technologies LLC's Complaint; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 124; filed Sep. 7, 2010; 11 pages.

- Defendant McAfee, Inc.'s Answer and Counterclaim to Prism's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 131; filed Sep. 10, 2010; 11 pages.
- Defendant The Mathworks, Inc.'s First Amended Answer and Counterclaim to Prism's Complaint for Patent Infringement; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220; Doc. No. 133, filed Sep. 13, 2010; 11 pages.
- Request for Ex Parte Reexamination of U.S. Patent No. 7,290,288, dated Apr. 8, 2010, pp. 1-288; Exhibit AA, 7 pages; Exhibit L, 43 pages; Exhibit M, 54 pages; Exhibit N, 84 pages; Exhibit O, 63 pages; Exhibit P, 41 pages; Exhibit Q, 29 pages; Exhibit R, 14 pages; Exhibit S, 13 pages; Exhibit T, 13 pages.
- Abadi et al.; Authentication and Delegation with Smart-Cards; Jul. 1992; 30 pages.
- Aboba, B., et al.; "Radius Authentication Client MIB;" Request for Comments: 2618; Jun. 1999, 14 pages.
- Ahuja, V.; Network and Internet Security; 1996; 147 pages.
- Anderson et al.; RFC 68.2—DCE 1.2.2 Public Key Login—Functional Specification; Feb. 1996; 44 pages.
- Anderson et al.; RFC 68.3—DCE 1.2.2 Public Key Login—Functional Specification; Jan. 1997, 112 pages.
- Anderson et al.; RFE 68.1—DCE 1.2 Public-Key Login—Functional Specification; Feb. 1995; 62 pages.
- Andreessen, M.; Interoperable Security; Dec. 1996; 2 pages.
- Andrews, Whit; Content Sites Vexed by Password Abuse, Reprinted from Web Week, vol. 3, Issue 4; Feb. 17, 1997; 3 pages.
- Andrews, Whit; out with the old . . . ; Old Guard of Content Providers Adopt to the Web; Reprinted from Web Week, vol. 2, Issue 20; Dec. 16, 1996; 3 pages.
- Arseniev, M.; How are X.509 Certificates Used in User Authentication and Authorization? Feb. 2002; 1 page.
- Atkinson, R.; RFC 1826—IP Authentication Header; Aug. 1995; 13 pages.
- Atkinson, R.; RFC 1827—IP Encapsulating Security Payload (ESP); Aug. 1995; 12 pages.
- Baker et al.; RFC 2082—RIP-2 MD5 Authentication; Jan. 1997; 12 pages.
- Battelle; Battelle Annual Press Release for 1996; "Battelle, Cybermark Complete Successful Testing of Digital Cash Transfer from Smart Card;" generated from <http://www.battelle.com/annualreports/ar96/digital.htm> on Feb. 7, 2007; Battelle Memorial Institute; (VERI-1607108-VERI-1607110).
- Battelle; Solutions Update; Technology Development, Product Development, and Technology Commercialization; The chemical industry pools environmental technology dollars; Fall 1996; (VERI-1607111-VERI-1607122).
- Berners-Lee, T., et al.; "Hypertext Transfer Protocol—HTTP/1.0;" Request for Comments: 1945; May 1996; 60 pages.
- Bowen, Barry D.; How Popular Sites Use Cookie Technology; Shopping baskets are a natural use for cookies, but uncovered several surprising uses, too; Netscape World; Apr. 1997; 13 pages.
- Braden, R., et al.; RFC 1636—Report of IAB Workshop on Security in the Internet Architecture; Jun. 1994; 49 pages.
- Braden, R.; "Requirements for Internet Hosts—Communication Layers;" Request for Comments: 1122; Oct. 1989; 116 pages.
- Bridges, S.; Strong Authentication Questions; Mar. 1996; 3 pages.
- Bruno, Lee; "Software & Security Netegrity's Sideminder Software Lets Net Managers Get Centered on Security;" Data Communications, vol. 26, No. 1; Jan. 1997; 2 pages.
- Bryant, Bill; "Designing an Authentication System: a Dialogue in Four Scenes;" Massachusetts Institute of Technology; Feb. 1997; 18 pages.
- BTAS and the World Wide Web: An Introduction and Technical Overview; DRAFT; Apr. 1997; pp. 1-23.
- Burati, M., et al.; "User-to-User Authentication—Functional Specification;" Request for Comments: 91.0; Jan. 1996; 9 pages.
- Business Wire; Secure Computing Announces Immediate Availability of Sidewinder 3.0; Security Server Employs Fully Integrated Perimeter Security, Ipsec Interoperable Encryption, Strong User Authentication, and E-mail Content Filtering. Sep. 17, 1996; 2 pages.
- Business Wire; Secure Computing Corp. Announces Agreement with Security Dynamics Technologies, Inc. to Provide Enhanced Security for Computer Networks; Jan. 23, 1996; 2 pages.
- Byte; Kay, Russell, Jun. 1994/Special Report/Distributed and Secure; "When you distribute information and processing, you also delegate security responsibility. Good access controls, eyes-open administration, and communications encryption can make all the difference." BYTE.com; CMP Media LLC; (VERI-1605576-VERI-1605587).
- Carr, J.; The Price of Access is Eternal Vigilance—Security Sells Itself as Remote Connections Spread the Risk of Unauthorized Access to Corporate Data; Oct. 1995; 4 pages.
- CCITT/ISO; Information Technology—Open Systems Interconnection—The Directory: Overview of Concepts, Models and Services; Dec. 2001; 30 pages.
- Choudhury, A., et al.; Copyright Protection for Electronic Publishing Over Computer Networks, IEEE Network; May/Jun. 1995; pp. 12-20.
- Chrysalis; Chrysalis-ITS; Canadian Department of National Defense Installs Integrated Information Security solutions from Chrysalis; Mergent International, and Northern Telecom (Nortel) Top Information Security Vendors Combine Solutions to Provide a High Level of Security to DND in Ottawa; Rocky Hill, Conn. (Apr. 19, 1996); (VERI-1605384-VERI-1605385).
- Chrysalis; Chrysalis-ITS; Safeguarding the Keys to Electronic Commerce; Chrysalis-ITS, Inc.; (VERI-1605091-VERI-1605092), 1997.
- Chrysalis; Seminerio, Maria; Chrysalis-ITS; Chrysalis to debut encryption token card; PC Week Online Oct. 30, 1996 (reprinted); (VERI-1605093-VERI-1605094).
- Cisco Systems, Inc.; Single-User Network Access Security TACACS+; Mar. 1995; 8 pages.
- Coe, et al. D.; Developing and Deploying Corporate Cryptographic Systems; Jul. 1995; 13 pages.
- Communication News; NSA Provides Value-Added Crypto Security; May 1995; 2 pages.
- Communications News; New Product Information: Dec. 1996; (VERI-1606981-VERI-1606933).
- Community Connexion, Inc.; Stronghold Version 1.3 User's Guide; Community Connexion, Inc.; 1996; (CA956585-CA956614).
- Community Connexion; Mailing list archives; Community Connexion Announces Stronghold Version 1.2; Community Connexion, Inc.; Jul. 16, 1996.
- COMP.SECURITY.UNIX; password encryption (security) over networks, Google Groups; Jun. 1994.
- COMP.SECURITY.UNIX; secure ID cards; which is best?; Google Groups; Oct. 1994; (VERI-1605401-VERI-1605404).
- Compuomatic Secure Networks GmbH; CryptoGuard VPN System, Secured Connections via Shared Infrastructures; 2005; 13 pages.
- Constance, Paul; DISA Buys 180,000 Licenses for Navigator, Government Computer News; Jul. 1996; 2 pages.
- Croes, T.; LAN access worlds Converge; Once-competing vendor camps are now borrowing from each other as business and Internet communities find common ground; Oct. 1995; 4 pages.
- CryptoSwift; CryptoSwift Developer Frequently Asked Questions; Mar. 1997; 3 pages.
- CryptoSwift; CryptoSwift Secure Server Accelerator Frequently Asked Questions; Apr. 1997; 7 pages.
- Csinger, Andrew; Letters to the Editor; Certification: Up and Running; (Reprinted from Web Week, vol. 2, Issue 18, Nov. 18, 1996; (CA956617).
- Csinger, Andrew; Technology B.C. Application Form; InterSpect Systems Consulting Corp; OpenMed; a secure authentication protocol for health care information transaction; (CA956562-CA956584), 1997.
- CTI; Letter to Roger Loyer with attachment (Electronic Distribution Facility: Response to BayBank Systems—Request for Proposal; Corporate Technologies, Inc.; Feb. 12, 1996; (CA955582-CA955597).
- Curtin, Matt; Introduction to Network Security; Mar. 1997; 16 pages.
- Cybermark; CyberMark appoints chairman, CEO; Columbus Business First; Dec. 27, 1996; American City Business Journals Inc.: (VERI-1607123).

- Cybermark; Frees, John; CEO Graham sees Cybermark as a "smart" career move; Columbus Business First; Jan. 3, 1997; American City Business Journals Inc. (VERI-1607124-VERI-1607125).
- Cyberstore Systems Inc., et al.; InterMed and OpenMed: Open Systems for Secure Health Care Information Transaction; Mar. 31, 1995; (CA956497-CA956503).
- Cyberstore Systems Inc., et al.; OpenMed: Open Systems for Secure Health Care Information Transaction; OpenMed Business Plan; Jul. 29, 1995; (CA956469-CA956496).
- Cyberstore; Certification Authority; (CA956518-CA956528), 1997.
- Dascom; "Integration of DCE/Kerberos with Public Key Infrastructure using the Cryptographic Message Syntax (PKINIT/CMS); Mar. 30, 1998; 27 pages.
- Davis, Beth; Digital Certificate Options Offered; TechwebNews; CMP Media Inc.; Jan. 27, 1997; (CA956616).
- Davis, Beth; Security Check—Digital certificates slow to gain users, despite strides; TechwebNews; CMP Media Inc.; Feb. 10, 1997; (CA956615).
- Davis, R.; Network Authentication Tokens; Dec. 1989; pp. 234-238.
- de Laat, C., et al.; Generic AAA Architecture; Request for Comments: 2903; Aug. 2000; 26 pages.
- Doan, Amy; "Remote Access Vendors Try Radius;" InfoWorld; Sep. 23, 1996; 1 page.
- Duffy, J.; Livingston gets into Net game with new wares; Aug. 1995; 1 page.
- E-Mail Responses by various; LDAP for logon?; May 1996; (CA133836-CA133842).
- E-Mail Responses by various; strong authentication questions; Mar.-May 1996; (CA134275-CA134277).
- EMV '96; Chip Electronic Commerce Specification, Version 1.0; Dec. 1999; 69 pages.
- Entrust; Curry, Ian; Entrust Technologies; Entrust® Key Management Overview; Apr. 1996, Version 1.4; Entrust Technologies; (VERI-1605756-VERI-1605762).
- Entrust; Entrust Technologies White paper; Implementing Cryptoki Libraries for Entrust®; Jun. 1997; Version 1.2; Entrust Technologies; (VERI-1605386-VERI-1605400).
- Entrust; Entrust Technologies; Team Profiles; Entrust Technologies; (VERI-1605595-VERI-1605599), 1997.
- Entrust; Press Release; Apple, IBM, JavaSoft, Motorola, Netscape, Nortel, Novell, RSA, and Silicon Graphics Announce PICA Crypto-Alliance; Redwood City, Calif.; Oct. 17, 1996; Northern Telecom; (VERI-1604986-VERI-1604989).
- Entrust; Press Release; Choro Systems and Northern Telecom (Nortel) Secure Networks Group Sign VAR Agreement; Ottawa, Canada; Aug. 28, 1995; Northern Telecom; (VERI-1604930-VERI-1604932).
- Entrust; Press Release; Cowboys Call on Northern Telecom (Nortel) to Quarterback "Dallas Cowboys Online"; Dallas; Sep. 6, 1996; Northern Telecom; (VERI-1604981-VERI-1604983).
- Entrust; Press Release; Devon Software Corp. Announces Kyberpass the First User Authenticating Firewall to Incorporate Northern Telecom's (Nortel) Entrust Data Security Software; Ottawa, ON; Feb. 14, 1996; Northern Telecom; (VERI-1604952-VERI-1604954).
- Entrust; Press Release; Digital Equipment Corporation to Resell Entrust Technologies' Enterprise Security Products; Ottawa, Apr. 29, 1997; Northern Telecom; (VERI-1605029-VERI-1605031).
- Entrust; Press Release; Entrust Strengthens Data Security for Microsoft Exchange; Philadelphia; Apr. 7, 1997; Northern Telecom; (VERI-1605023-VERI-1605024).
- Entrust; Press Release; Entrust Technologies Demonstrates Interoperability with Multiple Secure E-Mail Products; Philadelphia; Apr. 7, 1997; Northern Telecom; (VERI-1605018-VERI-1605020).
- Entrust; Press Release; Entrust Technologies Launches Partner Program; Ottawa; Jan. 27, 1997; Northern Telecom; (VERI-1605010-VERI-1605014).
- Entrust; Press Release; Entrust Technologies Names John Ryan CEO and Announces Headquarters; San Francisco; Jan. 27, 1997; Northern Telecom; (VERI-1605008-VERI-1605009).
- Entrust; Press Release; Entrust Technologies Now Shipping Entrust/WebCA and Entrust/ICE; Philadelphia; Apr. 7, 1997; Northern Telecom; (VERI-1605021-VERI-1605022).
- Entrust; Press Release; Entrust Technologies Sweeps Prestigious Awards at NetWorld+Interop; Las Vegas; May 7, 1997; Northern Telecom; (VERI-1605032-VERI-1605033).
- Entrust; Press Release; Entrust Technologies Unveils Entrust/ICE Desktop Encryption Product; Jan. 27, 1997; Northern Telecom; (VERI-1605002-VERI-1605003).
- Entrust; Press Release; Entrust Technologies? 3.0 Offers Users and Network Managers Unmatched Security and Greater Flexibility; Ottawa; Jun. 2, 1997; Northern Telecom; (VERI-1605036-VERI-1605038).
- Entrust; Press Release; Entrust Technologies? New Toolkit Will Accelerate Deployment of Internet Applications; Ottawa, Apr. 28, 1997; Northern Telecom; (VERI-1605025-VERI-1605028).
- Entrust; Press Release; Entrust wins SCOAP awards of excellence; Ottawa; May 7, 1996; Northern Telecom; (VERI-1604964-VERI-1604967).
- Entrust; Press Release; Entrust® Technologies' CAST Encryption Algorithm Now Available for Free Commercial and Non-commercial Use; Ottawa; Jan. 24, 1997; Northern Telecom (VERI-1604999-VERI-1605001).
- Entrust; Press Release; Harbinger Chooses Nortel to Provide Security for Electronic Commerce Solutions Entrust-aware Product List Continues to Grow; Chicago, Illinois; May 15, 1996; Northern Telecom; (VERI-1604970-VERI-1604971).
- Entrust; Press Release; Hewlett-Packard to use Nortel's Data Security Technology; Ottawa; Aug. 27, 1996; Northern Telecom; (VERI-1604979-VERI-1604980).
- Entrust; Press Release; Hewlett-Packard Turns to Nortel for E-Mail Security Solution; San Francisco; Jan. 16, 1996; Northern Telecom; (VERI-1604947-VERI-1604948).
- Entrust; Press Release; IBM Adds Nortel's Entrust Security software to Its Internet-Commerce Portfolio; Somers, N.Y.; Aug. 1, 1996; Northern Telecom; (VERI-1604974-VERI-1604976).
- Entrust; Press Release; ICL and Nortel Announce Collaboration for Large-Scale Enterprise Network Security X.500 Directory Supports Entrust Security; Anaheim, California; Apr. 29, 1996; Northern Telecom; (VERI-1604955-VERI-1604956).
- Entrust; Press Release; Information Security Corporation and Entrust Technologies Announce SecretAgent to Work with Entrust; San Francisco; Jan. 27, 1997; Northern Telecom; (VERI-1605015-VERI-1605017).
- Entrust; Press Release; JetForm and Entrust Technologies Announce Worldwide Alliance to Provide Advanced Security Solutions for Forms-Based Workflow and Intranet Applications; San Francisco; Jan. 27, 1997; Northern Telecom; (VERI-1605004-VERI-1605007).
- Entrust; Press Release; Linmor Information Systems Management Integrates Nortel Security Services into Nebula Network Management System (NMS); Dec. 20, 1995; Northern Telecom, (VERI-1604944-VERI-1604946).
- Entrust; Press Release; Microsoft selects Northern Telecom's Entrust network security technology to provide security for Microsoft Exchange Server; Oct. 17, 1994; Nashville, TN; Northern Telecom; (VERI-1604911-VERI-1604912).
- Entrust; Press Release; Nortel (Northern Telecom) Forms Entrust Technologies to Focus on Enterprise Security Market; Dallas; Jan. 2, 1997; Northern Telecom; (VERI-1604996-VERI-1694998).
- Entrust; Press Release; Nortel and LJL Enterprises Team to Offer Scalable and Secure E-Mail; Ottawa, Dec. 12, 1995; Northern Telecom; (VERI-1604942-VERI-1604943).
- Entrust; Press Release; Nortel Endorses S/MIME Specification Company Developing Toolkit for Secure Messaging Applications; Anaheim, California; Apr. 30, 1996; Northern Telecom; (VERI-1604962-VERI-1604963).
- Entrust; Press Release; Nortel Introduces Next Generation Software for Secure Data Communications: Entrust 2.0 Designed for Greater Efficiency and Ease of Use; San Francisco; Jan. 16, 1996; Northern Telecom; (VERI-1604949-VERI-1604951).
- Entrust; Press Release; Nortel Issues Demonstration Certificates for Internet Products Free Certificates Enable SSL; San Jose; Apr. 30, 1996; Northern Telecom; (VERI-1604960-VERI-1604961).
- Entrust; Press Release; Nortel Issues Demonstration Certificates Available for Netscape Navigator 3.0; Chicago, Illinois; May 15, 1996; Northern Telecom; (VERI-1604968-VERI-1604969).

## US 8,387,155 B2

Page 7

- Entrust; Press Release; Nortel Provides Data Security Technology to PayPro Network; Jun. 5, 1996; Northern Telecom (VERI-1604972-VERI-1604973).
- Entrust; Press Release; Nortel Secure Networks Ships Version of Entrust Running on Windows, Macintosh and UNIX Platforms; Scalable Security Software Can be used Worldwide; Ottawa, Ontario; Jul. 31, 1995; Northern Telecom; (VERI-1604928-VERI-1604929).
- Entrust; Press Release; Nortel Security Services Added to TradeWave Internet Solutions; Integrated Security and Public Key Management Now Available from Single Internet Services Vendor; Austin, Texas; Sep. 25, 1995; Northern Telecom; (VERI-1604933-VERI-1604935).
- Entrust; Press Release; Nortel Unveils Next Level of Entrust Software for Secure Data Communications New Certificate Management Features Set Entrust 2.1 Apart; Ottawa, Aug. 19, 1996; Northern Telecom; (VERI-1604977-VERI-1604978).
- Entrust; Press Release; Nortel's Entrust Data Security Software Chosen by Canadian Government to Provide Public-Key Infrastructure; Ottawa; Sep. 16, 1996; Northern Telecom; (VERI-1004984-VERI-1604985).
- Entrust; Press Release; Northern Telecom (Nortel) and Milkyway Networks Introduce Security Solution to Business Internet Users; Ottawa; Nov. 7, 1995; Northern Telecom; (VERI-1604939-VERI-1604941).
- Entrust; Press Release; Northern Telecom (Nortel) and Tandem Sign Agreement Adding Entrust Security Technology to Tandem's Internet Commerce Offering; Ottawa; Nov. 15, 1996; Northern Telecom (VERI-1604994-VERI-1604995).
- Entrust; Press Release; Northern Telecom (Nortel) First in North America to Receive Computer Security Validation: Entrust Certified by U.S. and Canadian Agencies; Baltimore, Md; Oct. 10, 1995; Northern Telecom; (VERI-1604936-VERI-1604938).
- Entrust; Press Release; Northern Telecom (Nortel) Introduces Web-Based Security Software Product Entrust/WebCA Enables Web Session Security; Dallas; Nov. 11, 1996; Northern Telecom; (VERI-1604992-VERI-1604993).
- Entrust; Press Release; Northern Telecom and ZOOMIT Corporation Announce Secure Encryption and Authentication for Windows-Based LAN E-Mail Applications; Mar. 22, 1994; Nashville, Tenn.; Northern Telecom; (VERI-1604908-VERI-1604910).
- Entrust; Press Release; Northern Telecom introduces network security solution to safeguard data privacy and authenticity; Mar. 22, 1994; Washington, D.C.; Northern Telecom; (VERI-1604906-VERI-1604907).
- Entrust; Press Release; Northern Telecom's Entrust Network Security Product to Support National Semiconductor's iPower PersonaCard Hardware Token; Nov. 29, 1994; Boston, Mass.; Northern Telecom; (VERI-1604913-VERI-1604914).
- Entrust; Press Release; NYCE Chooses Nortel's Entrust as Network Security Solution Software; Dallas; Oct. 29, 1996; Northern Telecom; (VERI-1604990-VERI-1604991).
- Entrust; Press Release; Salomon Brothers Chooses Entrust Product Suite as Data Security Solution; New York; May 27, 1997; Northern Telecom; (VERI-1605034-VERI-1605035).
- Entrust; Press Release; Symantec and Nortel Team to Provide Secure Electronic Forms for Enterprises; Anaheim, California; Apr. 29, 1996; Northern Telecom; (VERI-1604957-VERI-1604959).
- Entrust; Press Releases; Control Data adds Nortel (Northern Telecom) Secure Networks' public-key security product to message integration solution; Entrust to provide Mail\*Hub with security services for electronic commerce; New Orleans, LA; May 8, 1995; Northern Telecom; (VERI-1604919-VERI-1604921).
- Entrust; Press Releases; Department of National Defence awards contract to Northern Telecom and ZOOMIT for secure e-mail system; Toronto, Ontario; Mar. 22, 1995; Northern Telecom; (VERI-1604917-VERI-1604918).
- Entrust; Press Releases; New network security system provides private, secure data communications using Nortel's Entrust product; Ottawa, May 15, 1995; Northern Telecom; (VERI-1604925-VERI-1604927).
- Entrust; Press Releases; Northern Telecom licenses security token technology from Chrysalis IIS for hardware extensions to Entrust network security; Redwood Stores, CA; Jan. 9, 1995; Northern Telecom; (VERI-1604915-VERI-1604916).
- Entrust; Press Releases; Shana and Nortel (Northern Telecom) Secure Networks announce Informed's support for Entrust; Collaboration offers authentication for Macintosh and Windows forms; New Orleans; LA; May 8, 1995; Northern Telecom; (VERI-1604922-VERI-1604924).
- Erdos, Marlena E., et al.; "Extending the OSF DCE Authorization System to Support Practical Delegation;" to appear in PSRG Workshop on Network and Distributed System Security; Feb. 11-12, 1993; 8 pages.
- Estrin, Deborah, et al.; "Visa Scheme for Inter-Organization Network Security;" IEEE Symposium on Security and Privacy; Apr. 1987; pp. 174-183.
- European Search Report dated Nov. 3, 2004 of European Application No. 01112859.2; (VERI-1606092-VERI-1606094).
- Farrell, S., et al.; AAA Authorization Requirements; Request for Comments: 2906; Aug. 2000; 23 pages.
- Federal Computer Week; Advertisement; FCW.COM; 4 pages; Apr. 10, 2000.
- Federal Computer Week; Elizabeth Sikorovsky; Xcert aims to simplify public key infrastructure. (Xcert Software's Sentry Certification Authority data security software) (Product Announcement); vol. 10, Issue 17, Jul. 1, 1996; (CA956511).
- Finseth, C.; RFC 1492—An Access Control Protocol, Sometimes Called TACACS; Jul. 1993; 21 pages.
- Fischer International; Smarty; Smarty™ Smart Card Reader; Executive Summary; Fischer International Systems Corporation; 1996-1997; (VERI-1606164-VERI-1606174).
- Ford, Warwick; Computer Communications Security: Principles, Standard Protocols and Techniques; PTR Prentice Hall; 1994; (CA956622-CA957126).
- Franks, et al.; RFC 2069—An Extension to HTTP: Digest Access Authentication; Jan. 1997; 17 pages.
- Freier, et al.; The SSL Protocol Version 3.0 draft-freier-ssl-version3-02.txt; Nov. 1996; 59 pages.
- Freier, et al.; The SSL Protocol Version 3.0, Internet Draft; Mar. 1996; 32 pages.
- Freier, et al.; The SSL Protocol Version 3.0; Mar. 1996; 60 pages.
- Fruth, P.; Product Update: CE Software Ouickmail 3.5; Nov. 1995; 3 pages.
- Galvin, Peter; Practicing what I preach: How I set up a secure e-commerce site; Security: Pete's Wicked World; Mar. 1997; (CA957611-CA957615).
- Galvin, Peter; Trials and tribulations of building an e-commerce server; Security: Pete's Wicked World; Apr. 1997; (CA955821-CA955828).
- Gaskell, et al.; RFC 71.0—Improved Security for Smart Card Use in DCE; Open Software Foundation Request for Comments 71.0; Feb. 1995; 9 pages.
- Gaskell, Gary Ian; "Integrating Smart Cards into Kerberos;" Feb. 2000; 128 pages.
- Gauntlet™ 3.1 for IRIX™ Administrator's Guide for !IRIX 5.3; Document No. 007-2826-002; Silicon Graphics, Inc.; 1996; (CA954783-CA955015).
- Gauntlet™ 3.1.1 for IRIX™ 6.2 Administrator's Guide; Document No. 007-2826-003; Silicon Graphics, Inc.; 1996; (CA955016-CA955263).
- GE Information Services; New Generations of Secure Internet Commerce Unveiled by GE Information Services; GE Information Services; Feb. 6, 1996; (CA955607-CA955609).
- Gifford, et al.; Payment Switches for Open Networks; Jul. 1995; 8 pages.
- Gligor, Virgil D., et al.; "On Inter-realm Authentication in Large Distributed Systems;" Proceedings of the 1992 IEEE Symposium on Security and Privacy; 1992, pp. 2-17.
- Global.H—RSAEURO types and constants; J.S.A. Kapp 1994-1996; (VERI-0015459-VERI-0015460).
- Going Public the IPO Reporter; Securities Data Publishing; vol. 20, Issue 39; Sep. 23, 1996; (CA956278-CA956328).
- Goldberg, D.; The MITRE User Authentication System; Aug. 1990; 6 pages.

TX0002-0009

Appx183

## US 8,387,155 B2

Page 8

- Haller, N., et al.; RFC 1704—On Internet Authentication; Oct. 1994; 16 pages.
- Haller, N.; RFC 1760—The S/KEY One-Time Password System; Feb. 1995; 12 pages.
- Harrel, Heather; V-ONE launches its new federal division; FCW. COM; Mar. 3, 1997; (CA957465-CA957466).
- Hinnebusch, Mark; Z39.50 Implementors Workshop; Aug. 8, 1996; (CA956529-CA956531).
- Hornstein, Ken; “Kerberos FAQ, v2.0;” <http://wwwfags.org/faqs/kerberos-faq/general/>; Sep. 17, 2009; 51 pages.
- Howes et al.; CITI Technical Report 95-7; A Scalable, Deployable Directory Service Framework for the Internet; Jul. 1995; 12 pages.
- Howes, et al.; RFC 1823—The LDAP Application Program Interface; Aug. 1995; 21 pages.
- Howes, et al.; The LDAP URL Format (Internet Draft); Draft-ietf-asid-idapv3-url-00.txt; Mar. 1997; 5 pages.
- Howes, T.; An X.500 and LDAP Database: Design and Implementation; Dec. 2003; 9 pages.
- Howes, T.; CITI Technical Report 95-8; The Lightweight Directors Access Protocol: X.500 Lite; Jul. 1995; 11 pages.
- Hunwick, T.; RFC 8.2—Security Requirements for DCE; Aug. 1996; 64 pages.
- IBM; Introduction to DCE; 1996; 9 pages.
- IBM; Presentation at the Securities Industry Middleware Council re DCE RFC 68.4 Update; Feb. 1999; 13 pages.
- InfoDev-Security.net; Chapter 5. Identification and Authentication; 2003; 32 pages.
- Interlink AAA Server Software: Authentication Guide; “LDAP and ProLDAP;” 2000; 16 pages.
- Interlink Networks AAA Server; “Administrator’s Guide;” 2000; 88 pages.
- Interlink Networks AAA Server; “Getting Started;” 2000; 31 pages.
- IRE; IRE and CyberGuard Announce Virtual Private Network Security Solution for Enabling Low Cost Internet Business Communication; SafeNetEnterprise—Enables the Secure Use of Public Networks for Private Business Transactions; Atlanta, GA (Sep. 17, 1996); Information Resource Engineering, Inc.; (VERI-1606027-VERI-1606029).
- IRE; News Release; Dan Mosley Joins IRE Advisory Board; Baltimore, Maryland; Mar. 10, 1997; Information Resource Engineering; (VERI-1605847-VERI-1605848).
- IRE; News Release; Former United States Treasury Secretary to Chair IRE Advisory Board; Baltimore, Maryland; Feb. 5, 1997; Information Resource Engineering; (VERI-1605855-VERI-1605856).
- IRE; News Release; France Telecom’s Nexus International Joins IRE to Expand Brazil’s Network Security Market; Baltimore, Maryland; Nov. 18, 1997; Information Resource Engineering; (VERI-1605883-VERI-1605884).
- IRE; News Release; Industry Executive joins IRE to Lead OEM Effort; Interest in Low-Cost SafeNet Technology Results in New Sales Channel; Baltimore, Maryland; Sep. 17, 1997; Information Resource Engineering; (VERI-1605808-VERI-1605809).
- IRE; News Release; Internet Security for the Millennium Available Now; Year 2000 Compliance Makes SafeNet™ the Security Solution for Tomorrow’s Electronic Business; Baltimore, Maryland; Dec. 4, 1997; Information Resource Engineering; (VERI-1605845-VERI-1605846).
- IRE; News Release; IRE adds International Sales VP; Baltimore, Maryland; Nov. 12, 1996; Information Resource Engineering; (VERI-1605869).
- IRE; News Release; IRE and Analog Devices to Provide Low-Cost, Secure Communications Chip for Electronic Commerce; Jan. 9, 1997; Information Resource Engineering; (VERI-1605857-VERI-1605859).
- IRE; News Release; IRE and Cyberguard Partner to Provide Complete Security Solution for Internet Business Communication; Aug. 8, 1996; Information Resource Engineering; (VERI-1605880-VERI-1605882).
- IRE; News Release; IRE and Lockheed Martin IS&T Form Strategic Alliance to Offer Turn-Key Secure Electronic Commerce; Jul. 16, 1997; Information Resource Engineering; (VERI-1605817-VERI-1605818).
- IRE; News Release; IRE and MCI Announce Sales and Marketing Agreement for Secure Internet Products and Services; Nov. 14, 1996; Information Resource Engineering; (VERI-1605867-VERI-1605868).
- IRE; News Release; IRE Announces Montgomery Securities as Investment Banking Adviser and Market Maker; Baltimore, Maryland; Jan. 6, 1997; Information Resource Engineering; (VERI-1605862).
- IRE; News Release; IRE Announces New Chief Financial Officer; Baltimore, Maryland; Jul. 21, 1997; Information Resource Engineering; (VERI-1605816).
- IRE; News Release; IRE Debuts SafeNet™ Partner Program; Increases Availability of Industry-Leading Internet Security Solutions; Information Resource Engineering; Baltimore, Maryland; Oct. 21, 1997; (VERI-1605899-VERI-1605900).
- IRE; News Release; IRE Demonstrates Standard Compliant/Public Key Leadership for Internet Virtual Private Networks; Industry test shows SafeNet/Enterprise capable of secure Internet interoperability; Baltimore, Maryland; Feb. 11, 1997; Information Resource Engineering; (VERI-1605853-VERI-1605854).
- IRE; News Release; IRE Frame Relay Encryptor Makes Business on High Speed Computer Networks a Reality; SafeNet/Frame Currently Showcasing at NetWorld+Interop; Baltimore, Maryland; May 8, 1997; Information Resource Engineering; (VERI-1605827-VERI-1605828).
- IRE; News Release; IRE Introduces Encryption Software for Windows; Baltimore, Maryland; Apr. 24, 1997; Information Resource Engineering; (VERI-1605834-VERI-1605835).
- IRE; News Release; IRE Products to Secure Virtual Banking System in Argentina; Baltimore, Maryland; Aug. 6, 1997; Information Resource Engineering; (VERI-1605814-VERI-1605815).
- IRE; News Release; IRE Receives Patent for Secure Portable Modem; Baltimore, Maryland; Sep. 9, 1996; Information Resource Engineering; (VERI-1605878-VERI-1605879).
- IRE; News Release; IRE Reports 1996 Financial Results; Baltimore, Maryland; Mar. 24, 1997; Information Resource Engineering; (VERI-1605839-VERI-1605840).
- IRE; News Release; IRE Reports Improved Financial Results; Baltimore, Maryland; Mar. 12, 1997; Information Resource Engineering; (VERI-1665815-VERI-1605826).
- IRE; News Release; IRE Reports Strong Financial Growth; Baltimore, Maryland; Aug. 11, 1997; Information Resource Engineering; (VERI-1605812-VERI-1605813).
- IRE; News Release; IRE Reports Third Quarter Results; Baltimore, Maryland; Nov. 14, 1996; Information Resource Engineering; (VERI-1605865-VERI-1605866).
- IRE; News Release; IRE SafeNet Products Protect Consumer Credit Applications on the Internet; Baltimore, Maryland; Sep. 3, 1997; Information Resource Engineering; (VERI-1605810-VERI-1605811).
- IRE; News Release; IRE SafeNet™ Products to Protect GTE’s Internet-based Crime Fighting Service; Information Resource Engineering; Baltimore, Maryland; Oct. 29, 1997; (VERI-1605897-VERI-1605898).
- IRE; News Release; IRE ships 3,000<sup>th</sup> SafeNet? product for secure Intranet use; Baltimore, Maryland; May 23, 1996; Information Resource Engineering; (VERI-1605800-VERI-1605801).
- IRE; News Release; IRE Significantly Expands Distribution in Latin America; Adds Eight Major Distribution Channels; Baltimore, Maryland; Jun. 3, 1997; Information Resource Engineering; (VERI-1605819-VERI-1605820).
- IRE; News Release; IRE Smartcard/Readers to be Used in U.S. Treasury Electronic Check Pilot Program; Baltimore, Maryland, Oct. 8, 1997; Information Resource Engineering; (VERI-1605804-VERI-1605805).
- IRE; News Release; IRE Subsidiary Introduces Highly Secure Frame Relay Encryptor for Computer Transmissions; Both 128-bit and DES Algorithms Are Offered; Baltimore, Maryland; Mar. 12, 1997; Information Resource Engineering; (VERI-1605843-VERI-1605844).
- IRE; News Release; IRE Subsidiary Wins Contract; Will Secure Swiss Electronic Payment System; Baltimore, Maryland; Nov. 12, 1997; Information Resource Engineering; (VERI-1605893-VERI-1605894).

TX0002-0010

Appx184

- IRE; News Release; IRE Takes Lead in Building Secure Foundation for Electronic Commerce on the Internet; Partners with NIST to Develop Public Key Standards; Baltimore, Maryland; Jul. 24, 1996; Information Resource Engineering; (VERI-1605885-VERI-1605886).
- IRE; News Release; IRE to Expand Distribution Channels in the U.S.; Names New Sales Executive to Lead the Development; Baltimore, Maryland; May 20, 1997; Information Resource Engineering; (VERI-1605823-VERI-1605824).
- IRE; News Release; IRE to Penetrate Japanese Market Through Distribution Agreement with Kanematsu; Baltimore, Maryland; Mar. 31, 1997; Information Resource Engineering; (VERI-1605836-VERI-1605838).
- IRE; News Release; IRE to Produce Revolutionary Low-Cost Secure Communications Chip; Baltimore, Maryland; Jan. 9, 1997; Information Resource Engineering; (VERI-1605860-VERI-1605861).
- IRE; News Release; IRE to Showcase Low Cost Smartcard Security Token; Baltimore, Maryland; May 1, 1997; Information Resource Engineering; (VERI-1605832-VERI-1605833).
- IRE; News Release; IRE's Highly Secure Encryption Systems Now Available for Sale Worldwide; Company Receives Export Approval from Commerce Department; Baltimore, Maryland; Mar. 14, 1997; Information Resource Engineering; (VERI-1605841-VERI-1605842).
- IRE; News Release, IRE's Internet Security Center Now On-Line Appoints Dr. Garry Meyer as Managing Director; Baltimore, Maryland; Jul. 11, 1996; Information Resource Engineering; (VERI-1605887-VERI-1605888).
- IRE; News Release; IRE's Internet Security System Chosen as Best of Show Finalist for Interop 1996; Baltimore, Maryland; Sep. 16, 1996; Information Resource Engineering; (VERI-1605821-VERI-1605822).
- IRE; News Release; IRE's MCI Relationship Likely to Become Marketing Alliance; Baltimore, Maryland; Oct. 18, 1996; Information Resource Engineering; (VERI-1605870-VERI-1605871).
- IRE; News Release; IRE's SafeNet™ Products Achieve Interoperability in Industry Workshop; Baltimore, Maryland, Oct. 15, 1997; Information Resource Engineering; (VERI-1605802-VERI-1605803).
- IRE; News Release; SafeNet Certified as Providing Strongest Security for Internet; New Designation to Give IRE a Competitive Edge; Baltimore, Maryland; Nov. 24, 1997; Information Resource Engineering; (VERI-1605863-VERI-1605864).
- IRE; News Release; State of Maryland Services to Go On-Line Using IRE SafeNet™ Products; Vehicle Registration Among Government Services to be Available on the Internet; Baltimore, Maryland; Sep. 22, 1997; Information Resource Engineering; (VERI-1605806-VERI-1605807).
- IRE; News Release; Strong SafeNet™ Sales Result in Third Quarter Revenue Growth for IRE; Information Resource Engineering; Baltimore, Maryland; Nov. 6, 1997; (VERI-1605895-VERI-1605896).
- IRE; News Release; Sun Microsystems Internet Commerce Group and IRE to Link and Distribute Products for Secure Commerce on the Internet; Apr. 2, 1996; Information Resource Engineering; (VERI-1605891-VERI-1605892).
- IRE; News Release; TRW Purchases IRE Encryption Systems to Protect Treasury Communications Nationwide; Baltimore, Maryland; Feb. 13, 1997; Information Resource Engineering; (VERI-1605851-VERI-1605852).
- IRE; News Release; U.S. Robotics and IRE Team to Announce Industry's First Complete Remote Access and Encryption System for Individuals, Enterprises and the Internet; New Strategic Relationship, Including x2, Expected to Accelerate Electronic Commerce and Remote Access Over Internet and Public Networks; May 7, 1997; Information Resource Engineering; (VERI-1605829-VERI-1605831).
- IRE; News Release; U.S. Secret Service Using IRE's Secure Modem During Presidential Campaign; Baltimore, Maryland, Sep. 26, 1996; Information Resource Engineering; (VERI-1605874-VERI-1605875).
- IRE; News Release; U.S. Treasury Renews Contract With IRE for Secure Electronic Commerce System; IRE's Network Security Products in Use Since 1991; Baltimore, Maryland; Oct. 15, 1996; Information Resource Engineering; (VERI-1605872-VERI-1605873).
- IRE; News Release; Vint Cerf to Serve on IRE Advisory Board; Baltimore, Maryland; Feb. 18, 1997; Information Resource Engineering; (VERI-1605849-VERI-1605850).
- ISDN News; Livingston Launches ISDN Router, Too; May 1996; 1 page.
- ISO/IEC; X.509 Information Technology—Open Systems Interconnection—The Directory: Authentication Framework; 1993; 40 pages.
- Israel, et al.; Authentication in Office System Internetworks; ACM Transactions of Office Information Systems; vol. 1, No. 3; Jul. 1983; pp. 193-210.
- Itoi, et al.; CITI Technical Report 98-7; Smartcard Integration and Kerberos V5; Dec. 1998; 11 pages.
- ITU-T; Data Networks and Open System Communications Security; Information Technology—Open Systems Interconnection—Security Frameworks for Open Systems: Access Control Framework; ITU-T Recommendation X.812; International Telecommunication Union; 1996; (CA957547-CA957594).
- ITU-T; Data Networks and Open System Communications, Security; Information Technology—Open Systems Interconnection—Security Frameworks for Open Systems: Overview; ITU-T Recommendation X.810; International Telecommunication Union; 1996 (CA957470-CA957495).
- ITU-T; Data Networks and Open System Communications, Security; Information Technology—Open Systems Interconnection—Security Frameworks for Open Systems; Authentication Framework; ITU-T Recommendation X.811; International Telecommunication Union; 1996; (CA957496-CA957546).
- Janson, et al.; Safe Single-Sign-On Protocol with Minimal Password Exposure No-Decryption, and Technology-Adaptivity; Mar. 1995; 4 pages.
- Jeffcoate, et al.; Internet Security Strategies and Solutions; Sep. 1997; 23 pages.
- Jones, J., et al.; Securing the World Wide Web: Smart Tokens and Their Implementation; Dec. 1995; 15 pages.
- Kaufman, C.; RFC 1507—DASS, Distributed Authentication Security Service; Sep. 1993; 119 pages.
- Kemp, D.; The Public Key Login Protocol; <draft-kemp-auth-pklogin-01.txt>; Aug. 13, 1996; 18 pages.
- Kemp, D.; The Public Key Login Protocol; <draft-kemp-auth-pklogin-02.txt>; Nov. 26, 1996; 18 pages.
- Kent, Stephen Thomas; Encryption-Based Protection Protocols for Interactive User-Computer Communication Over Physically Unsecured Channels; Massachusetts Institute of Technology; Jun. 1976; (VERI-1605635-VERI-1605755).
- King, C.; Web-Access Authentication Using Radius: An intermediate method of secure exchanges on the Web; Aug. 1996; 5 pages.
- Kohl, et al.; RFC 1510—The Kerberos Network Authentication Service (V5); Sep. 1993; 105 pages.
- Kohl, John T., et al.; "The Evolution of the Kerberos Authentication Service;" appeared in Distributed Open Systems; 1994; 15 pages.
- Kohnfelder; Towards a Practical Public-Key Cryptosystem; May 1978; 54 pages.
- Kotanchik, J.; RFC 59.0—Kerberos and Two-Factor Authentication; Mar. 1994; 11 pages.
- Krajewski, Jr., et al.; Applicability of Smart Cards to Network User Authentication; Computing Systems; vol. 7, No. 1; 1994; pp. 75-89.
- Krishnamurthy, Sriekha, et al.; "Digital Security Forensics SiteMinder—A Portal Security Management Tool;" White Paper; Ver. No. 1.0; Mar. 18, 2002; 25 pages.
- Lai, et al.; Endorsements, Licensing, and Insurance for Distributed System Services; Information Services Institute University of Southern California; Nov. 1994; pp. 170-175.
- Lennon, et al.; Transaction Response Message Authentication (Des/Kp); Dec. 1983; 3 pages.
- Linn, J.; Practical Authentication for Distributed Computing; 1990; pp. 31-40.
- Linn, J.; RFC 1508—Generic Security Service Application Program Interface; Sep. 1993; 46 pages.
- Livingston Enterprises, Inc.; Radius Administrator's Guide; May 1997; 107 pages.

## US 8,387,155 B2

Page 10

- Livingston Enterprises, Inc.; Radius software documents; Dec. 1994-Apr. 1995; (VERI-1606882-VERI-1606980).
- Livingston Enterprises, Inc.; SecurID Installation; Sep. 1998; 8 pages.
- Lloyd, B.; RFC 1334—PPP Authentication Protocols; Oct. 1992; 15 pages.
- Looi, M., et al; Enhancing SESAMEV4 with Smart Cards; Sep. 1998; 11 pages.
- Lowry, J.; Location-Independent Information Object Security; IEEE; 1995; pp. 54-62.
- Lucent Technologies; “RADIUS Remote Authentication Dial in User Service;” Jun. 1999; 6 pages.
- Lucent Technologies; Radius Code from Lucent radiusd.c; RADIUS, Remote Authentication Dial in User Service; 1992-1999; Lucent Technologies Inc.; pp. 1-48; (VERI-1607419-VERI-1607466).
- Maddox, Kate; New Net Options for Business—Open Market touts safe, complete solutions; InformationWeek; Mar. 4, 1996; 1 page.
- McLaughlin; SunWorld News: Directory of the Month of Jun. 1996; 2 pages.
- McLaughlin; SunWorld News: New Products for the Week of May 27; Jun. 1996; 7 pages.
- Menezes, A., et al.; “Handbook of Applied Cryptography;” CRC Press, Inc.; 1997; cover page and pp. 1-319, 321-383, 365-541, 543-661 and 663-780.
- Merit AAA Server; “Differentiating Authentication Policy by Hunt Group;” printed Sep. 2009; 5 pages.
- Merit AAA Server; “Distributed Authentication/Authorization;” printed Sep. 2009; 3 pages.
- Merit AAA Server; “Installation Instructions for MichNet Dial-in;” printed Sep. 2009; 7 pages.
- Merit AAA Server; “LAS—Local Authorization Serve;” printed Sep. 2009; 6 pages.
- Metzger, et al.; RFC 1828—IP Authentication Using Keyed MDS; Aug. 1995; 6 pages.
- Micali, S.; Efficient Certificate Revocation; Mar. 1996; 10 pages.
- Miceli, S.; Enhanced Certificate Revocation System; 1995; 10 pages.
- Microsoft; The Microsoft Internet Security Framework: Technology for Secure Communication, Access Control, and Commerce; Dec. 1996; 9 pages.
- Miller, M.; When remote access needs to be blocked; Nov. 14, 1994; 2 pages.
- Mills, D.L.; RFC 1004—A Distributed Protocol Authentication Scheme; Apr. 1987; 8 pages.
- MISC.ACTIVISM.PROGRESSIVE; Horvitz, Robert; NATO support for key-escrow crypto (long); Google Groups; Nov. 1995; (VERI-1605777-VERI-1605793).
- Mullan, S.; “DCE Interoperability With Kerberos—Functional Specification;” Request for Comments: 92.0; Jan. 1996; 27 pages.
- Myers, et al.; Online Certificate Status Protocol, version 2; draft-ietf-pkix-ocspv2-00.txt; Sep. 2000; 20 pages.
- Myers, et al.; RFC 2560—X.509 Internet Public Key Infrastructure Online Certificate Status Protocol—OCSP; Jun. 1999; 22 pages.
- Myers, J.; RFC 1731—IMAP4 Authentication Mechanisms; Dec. 1994; 6 pages.
- N. Nagaratnam, et al.; Resource Access Control for an Internet User Agent; Jun. 1997; 11 pages.
- NameFLOW—Paradise—Quarterly Service Report Oct.-Dec. 1995; 26 pages.
- Naor, et al.; Certificate Revocation and Certificate Update; Jan. 1998; 13 pages.
- National Research Council, Computer Science and Telecommunications Board; Cryptography’s Role in Securing the Information Society; 1996; pp. i-xxx, 2 cover pages, and pp. 1-688.
- National Security Agency; Basic Certification Requirements for FORTEZZA—Enabled Applications; Version 1.1; Mar. 1997; 17 pages.
- National Security Agency; FORTEZZA—Certification Requirements for File Protection Applications, Version 1.04, Jan. 1996; 18 pages.
- National Security Agency; FORTEZZA Application Developer’s Documents, Version R1.0; Jun. 11, 1996; 77 pages.
- National Security Agency; FORTEZZA Application Implementors Guide for the PCMCIA Based FORTEZZA Cryptologic Card, Version 1.00; Jan. 1995; 94 pages.
- National Security Agency; FORTEZZA Application Implementors Guide for the PCMCIA Based FORTEZZA Cryptologic Card, Revision 1.01; Apr. 6, 1995; pp. i-v, 1-101, and A-1-A-3.
- National Security Agency; FORTEZZA Application Implementors Guide for the Fortezza Crypto Card ICD Revision P1.5 and the Fortezza Cryptologic Interface Programmers Guide, Revision 1.52; Mar. 5, 1996; 108 pages.
- National Security Agency; FORTEZZA Certification Requirements for World Wide Web Clients and Servers; Version 1.0; Dec. 1996; 13 pages.
- National Security Agency; FORTEZZA Cryptologic Interface Programmers Guide Revisions 1.52; Jan. 1996; 83 pages.
- National Security Agency; Fortezza Program Overview; Version 4.0a; Feb. 1996; 29 pages.
- National Security Agency; Interface Control Document for the Fortezza Crypto Card; Revision P1.5; Dec. 1994; 95 pages.
- National Security Agency; Mosaic Tessera document; prior to Aug. 29, 2002; 6 pages.
- Needham, et al.; Using Encryption for Authentication in Large Networks of Computers Networks; Communications of the ACM, vol. 21, No. 12; Dec. 1978; pp. 993-999.
- Nelson, Dave, et al.; “Current Meeting Report—Minutes of the Remote Authentication Dial-In User Services Working Group (radius),” Mar. 1996; 6 pages.
- Netegrity; “SiteMinder Frequently Asked Questions;” [http://web.archive.org/web/19990508041248/www.netegrity.com/product/siteminder\\_faq\\_s.html](http://web.archive.org/web/19990508041248/www.netegrity.com/product/siteminder_faq_s.html); May 8, 1999; 8 pages.
- Netegrity; NeTegrity Backgrounder; NeTegrity, Inc.; Feb. 1997; 4 pages.
- Netegrity; NeTegrity Unveils Industry’s First Enterprise-Wide, Integrated Network Security Management System; NeTegrity, Inc.; Oct. 15, 1996; 2 pages.
- Netegrity; NeTegrity, Inc. and Encotone Ltd. form U.S. Joint Venture to Market Acoustic Smart Card Technology; NeTegrity, Inc.; Nov. 4, 1996; (CA954771-CA954772).
- Netegrity; Netegrity™ SiteMinder™, Web Agent, Operations Guide for NT Version 2.0; Netegrity, Inc.; 1996-1997; (CA004932-CA004974).
- Netegrity; Netegrity™ SiteMinder™, Web Agent, Operations Guide for NT Version 1.0; Netegrity, Inc.; 1996-1997; (CA005007-CA005012).
- Netegrity; SiteMinder Authentication Server for Windows NT; NeTegrity, Inc.; 1996.
- Netegrity; SiteMinder Product/Technology Backgrounder; NeTegrity, Inc.; 1996; 3 pages.
- Netegrity; SiteMinder™ Security Manager; NeTegrity, Inc.; 1997; (CA954775).
- Netegrity; Software & Security; Netegrity’s Siteminder software lets net managers get centered on security; NeTegrity, Inc.; Jan. 1997; (CA954730-CA954732).
- Netscape; An Internet Approach to Directories; 1996; 20 pages.
- Netscape; Certificate-Mapping Programmer’s Guide; 1997; 73 pages.
- Netscape; FORTEZZA® CryptoSecurity Products; Oct. 1996; 22 pages.
- Netscape; Hitachi and Netscape to Collaborate on Intranet and Extranet Solutions Based on LDAP Standard for Internet Directories; Dec. 1997; 2 pages.
- Netscape; Introduction to Communicator; 1997; 178 pages.
- Netscape; Managing Netscape Servers—Netscape Administration Server 3.0; 1997; 92 pages.
- Netscape; More Than 40 Companies Join Netscape and U. Michigan to Support Lightweight Directory Access Protocol As Proposed Standard for Internet Directories; Apr. 1996; 4 pages.
- Netscape; Netscape Announces Netscape Certificate Server to Enable Companies to Encrypt Enterprise Communications and Data; Apr. 1996; 3 pages.
- Netscape; Netscape Announces Netscape Suitespot 3.0 for Open Email and Groupware on Intranets; Oct. 1996; 13 pages.

- Netscape; Netscape Certificate Server 1.0—A Powerful Certificate-Management Solution; 1996; 3 pages.
- Netscape; Netscape Certificate Server 1.0 FAQ; 1996; 6 pages.
- Netscape; Netscape Certificate Server Administrator's Guide for Unix; 1997; 269 pages.
- Netscape; Netscape Certificate Server Administrator's Guide for Windows NT; 1997; 264 pages.
- Netscape; Netscape Certificate Server Installation for Unix; 1997; 53 pages.
- Netscape; Netscape Certificate Server Installation for Windows NT; 1997; 48 pages.
- Netscape; Netscape Communicator Supports Smart Cards and Tokens So Mobile Users Can Safely Access Corporate Networks Remotely; Aug. 1997; 3 pages.
- Netscape; Netscape Directory Server 1.0—Server Software for Centralized Directory Management; 1996; 7 pages.
- Netscape; Netscape Directory Server 1.0 Data Sheet; 1996; 3 pages.
- Netscape; Netscape Directory Server 1.0 Fact Sheet; Dec. 1996; 2 pages.
- Netscape; Netscape Directory Server 1.0 FAQ; 1996; 5 pages.
- Netscape; Netscape Enterprise Server 3.0—Administrator's Guide for Windows NT; 1997; 302 pages.
- Netscape; Netscape Enterprise Server 3.0—Administrator's Guide for Unix; 1997; 300 pages.
- Netscape; Netscape Enterprise Server 3.0—The Enterprise-Strength Web Server for the Intranet; 1996; 7 pages.
- Netscape; Netscape Enterprise Server 3.0 FAQ; 1996; 4 pages.
- Netscape; Netscape Expands Mission Control to Provide Unified Administration of Intranets and Extranets with Lower Cost for Ownership; Dec. 1997; 3 pages.
- Netscape; Netscape Products With Fortezza Fact Sheet; Feb. 1997; 2 pages.
- Netscape; Netscape SuiteSpot—The Cost Effective and Full-Service Intranet Solution; 1996; 12 pages.
- Netscape; Netscape SuiteSpot 3.0 FAQ; 1996; 5 pages.
- Netscape; Netscape to Offer Fortezza Cryptographic Capability for its Software Products; Oct. 1995; 2 pages.
- Netscape; NSAPI Programmer's Guide—Netscape Enterprise Server Version 3.0; 1997; 180 pages.
- Netscape; Securing Communications on the Intranet and Over the Internet; Jul. 1996; 17 pages.
- Netscape; Securing Information Distribution Using Netscape Products with FORTEZZA®; 1996; 60 pages.
- Netscape; Single Sign-On Deployment Guide-Security; 1997; 94 pages.
- Netscape; SSL 2.0 Protocol Specification; Feb. 1995; 26 pages.
- Netscape; U.S. Department of Defense Signs Agreement for Netscape Client and Server Software; Oct. 1997; 2 pages.
- Netscape; Using Netscape Products with FORTEZZA; 1997; 42 pages.
- Netscape; Web Publisher User's Guide—Netscape Enterprise Server Version 3.0; 1997; 154 pages.
- Netscape; What the Press is Saying About Netscape's New Servers; 1996; 3 pages.
- Network Computing; Certificate Authorities: How Valuable Are They?; Apr. 1, 1997; (CA956512-CA956517).
- Neumann, Peter G.; Architectures and Formal Representations for Secure Systems; Computer Science Laboratory; SRI International EL-243; Oct. 2, 1995; Final Report; SRI Project 6401; (VERI-1605407-VERI-1605564).
- Newman, et al.; Kerberos: An Authentication Service for Computer Networks; reprinted from IEEE Communications Magazine, vol. 32, No. 9, pp. 33-38; Sep. 1994; 11 pages.
- Newsbytes News Network; GTE's CyberTrust for Web Electronic Commerce; Feb. 6, 1996; 4 pages.
- Newsbytes; UK—Security Dynamics Offers Remote Access Technology; Mar. 1996; 1 page.
- OASIS; Assertions and Protocol for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 47 pages.
- OASIS; Bindings and Profiles for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 31 pages.
- OASIS; Conformance Program Specification for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 23 pages.
- OASIS; Glossary for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 13 pages.
- OASIS; Security and Privacy Consideration for the OASIS Security Assertion Markup Language (SAML); OASIS Standard; Nov. 5, 2002; 26 pages.
- Oehler, et al.; RFC 2085—HMAC-MD5 IP Authentication with Replay Prevention; Feb. 1997; 6 pages.
- Open Market, Inc.; Open Market and iCat Strengthen Partnership; PRNewswire; Cambridge, Mass.; Apr. 8; (VERI-1605901-VERI-1605903), 1997.
- Open Market, Inc.; Open Market, Interleaf Team on Web "Secure Doc Mgt"; Washingtonpost Newsweek Interactive; Waltham, Massachusetts; Mar. 5, 1996; (VERI-1605905-VERI-1605906).
- Open Market, Inc.; Open Market's "3-Tier Architecture" for Web; Washingtonpost Newsweek Interactive; Waltham, Massachusetts; Mar. 14, 1996; (VERI-1605907-VERI-1605908).
- Oppen, et al.; The Clearinghouse: A Decentralized Agent for Locating Named Objects in a Distributed Environment; ACM Transactions on Office Information Systems, vol. 1, No. 3; Jul. 1983; pp. 230-253.
- Oracle; Secure Network Services Administrator's Guide Version 2.0; 1995; 136 pages.
- Parekh, Sameer; Re: WWW servers; Community ConneXion, Inc.; Jun. 6, 1996; (CA956618-CA956619).
- Parekh, Sameer; Re: WWW servers; Community ConneXion, Inc.; Jun. 6, 1996; (CA956620-CA956621).
- Parker, et al.; Sesame Technology Version 4 Overview; Issue 1; Dec. 1995; 90 pages.
- Pato, J.; "A Generic Interface for Extended Registry Attributes;" Request for Comments: 6.0; Jun. 1992; 23 pages.
- Pato, J.; "Extending the DCE Authorization Model to Support Practical Delegation (Extended Summary);" Request for Comments: 3.0; Jun. 1992; 18 pages.
- Pato, J.; "Hierarchical Trust Relationships for Inter-Cell Authentication;" Request for Comments: 7.0; Jul. 1992; 7 pages.
- Pato, J.; RFC 26.0—Using Pre-Authentication to Avoid Password Guessing Attacks; Open Software Foundation Request for Comments 26.0; Jun. 1993; 7 pages.
- Pato, Joseph N.; "Distributed Computing Environment (OSF DCE) Security Architecture;" 14 Forum; Jan. 18-27, 1993; 32 pages.
- Payserv; TBSS (Telematic Base Security Services); Approved procedures and mechanisms for the protection of electronic data communications; IBO 920 353 12.96; Version 1.2; Dec. 6, 1996; (VERI-1606053-VERI-1606091).
- PC Magazine Online; Netscape Shoots to Kill Microsoft and Lotus; Apr. 1996; 2 pages.
- Perkins, C.; RFC 2002—IP Mobility Support; Oct. 1996; 74 pages.
- PR Newswire; Secure Computing Launches Full Suite of Products for Enterprise Network Security; Solutions Encompass Perimeter Control, Access Control, Web Browser and Intrawall; Apr. 1996; 2 pages.
- RADIUS Server Source Code; Apr. 1995; 103 pages.
- Rainbow Technologies; iKey 1000 Series Developer's Guide; Jul. 2002; 30 pages.
- Rainbow Technologies; Sentinel SuperPro™—Securing the Future of Software Developer's Guide; 1991-1996; 83 pages.
- Rainbow Technologies; SentinelEve3™ Software Protection System Developer's Guide; 1989-1995; 98 pages.
- Rapoza, Jim; Sentry CA cross-checks certificates; Xcert uses LDAP directory secured via SSL for flexible authentication between authorities; PC Week Online; Apr. 16, 1997; 2 pages.
- Regents of the University of Michigan; The SLAPD and SLURPD Administrators Guide, University of Michigan, Release 3.3; Apr. 1996; 100 pages.
- Requests for Comments (RFC) submitted at the *Markman* hearing; Privacy Enhancement for Internet Electronic Mail: Part I: Message Encryption and Authentication Procedures (RFC: 1421, 40 pages) and Part II: Certificate-Based Key Management (RFC: 1422, 30 pages); Feb. 1993.
- Richard, Patrick C.; E-Mail Responses Re: certificates and CRLs—access and storage; Oct. 15, 1996; (CA134027-CA134028).

- Richard, Patrick; E-Mail Response Re: LDAP for logon?; May 22, 1996; (CA133800-CA133801).
- Richard, Patrick; Re: LDAP for logon?; May 21, 1996; (CA956532).
- Rigney, C., et al.; "RADIUS Accounting draft-ietf-radius-accounting-00.txt;" Jul. 1995; 22 pages.
- Rigney, C.; Current Meeting Report; Minutes of the Remote Authentication Dial in User Service BOF (RADIUS); Dec. 1995; 4 pages.
- Rigney, C.; RADIUS Accounting draft-ietf-radius-accounting-01.txt; Nov. 1995; 54 pages.
- Rigney, C.; RADIUS Accounting; draft-ietf-radius-accounting-02.txt; Feb. 1996; 46 pages.
- Rigney, C.; RADIUS Accounting; draft-ietf-radius-accounting-03.txt; May 1996; 50 pages.
- Rigney, C.; RADIUS Accounting; draft-ietf-radius-accounting-04.txt; Jun. 1996; 54 pages.
- Rigney, C.; RADIUS; BayLISA; Mountainview, California; Feb. 1996; 18 pages.
- Rigney, C.; RFC 2059—RADIUS Accounting; Jan. 1996; 50 pages.
- Roney, C.; RFC 2139—RADIUS Accounting; Apr. 1997; 25 pages.
- Rigney, et al.; RADIUS Extensions; draft-ietf-radius-ex-00.txt; Jan. 1997; 47 pages.
- Rigney, et al.; RADIUS Extensions; draft-ietf-radius-ext-01.txt; Sep. 1997; 46 pages.
- Rigney, et al.; RADIUS Extensions; draft-ietf-radius-ext-02.txt; Oct. 1998; 43 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-00.txt; May 1995; 70 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS) draft-ietf-radius-01.txt; Nov. 1995; 79 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS); draft-ietf-radius-radius-02.txt; Feb. 1996; 133.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS); draft-ietf-radius-radius-02.txt; May 1996; 78 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS); draft-ietf-radius-radius-03.txt; May 1996; 69 pages.
- Rigney, et al.; Remote Authentication Dial in User Service (RADIUS); Draft-ietf-radius-radius-04.txt; Jun. 1996; 138 pages.
- Rigney, et al.; RFC 2058—Remote Authentication Dial in User Service (RADIUS); Jan. 1997; 64 pages.
- Rigney, et al.; RFC 2138—Remote Authentication Dial in User Service (RADIUS); Apr. 1997; 66 pages.
- RISSS; Getting Connected; Regional Information Sharing Systems; Jun. 27, 2000; 16 pages.
- RISSS; Network Fundamentals; Regional Information Sharing Systems; Jun. 26, 2000; 17 pages.
- RISSTech; BJS/Search National Conference Justice; E-Government & the Internet Developing Security Policies and Procedures; Regional Information Sharing Systems; Jun. 27, 2000; (CA955648-CA955679).
- RISSTech; Federal CIO Council; XML Community of Practice; RISSSNET Trusted Credential Project; Regional Information Sharing Systems; Feb. 16, 2005; (CA955829-CA955842).
- Rodriguez, K.; New TCP/IP Products Unveiled at Expo; Aug. 1995; 3 pages.
- Rohland, B.; Token-Based Information Security for Commercial and Federal Information Networks; SPIE, vol. 2616; Mar. 1996; pp. 2-13.
- RSA; Baldwin, Robert; Using S/PAYTM; Jan. 30, 1997; RSA Data Security, Inc; (VERI-1605920-VERI-1606010).
- RSA; Ciphertext: The RSA Newsletter; vol. 4, No. 1, Spring 1996; RSA Data Security, Inc.; (CA955733-CA955740).
- RSA; S/PAYTM; RSA's Developer's Suite for Secure Electronic Transactions (SET); RSA Data Security, Inc.; 1996; (VERI-1606148-VERI-1606151).
- Rubin, A. D., et al.; Web Security Sourcebook; 1997; 187 pages.
- Rubin, A.D.; Independent One-Time Passwords, Proceedings of the Fifth USENIX UNIX Security Symposium; Jun. 1995; 11 pages.
- Ryan, G.; Making Netscape Compatible with FORTEZZA®—Lessons Learned; Aug. 1999; 27 pages.
- Salz, R.; RFC 100.0—DCE and FORTEZZA; Jan. 1997; 6 pages.
- Salz, R.; RFC 63.3—DCE 1.2 Contents Overview; Oct. 1996; 15 pages.
- Sars, C.; Unified Single Sign-On; Nov. 1998; 18 pages.
- Schneier, Bruce; Applied Cryptography—Protocols, Algorithms, and Source Code in C; 2nd ed.; 1996; 395 pages.
- Schroeder, W.; Kerberos/DCE, the Secure Shell, and Practical Internet Security; Oct. 1996; 10 pages.
- Schultz, T.; White Paper: Access Security with SecurID; Nov. 1999; 9 pages.
- Secure Computing Corp; 10-K—for Dec. 31, 1996; Annual Report—Form 10-K, SEC Info; (VERI-1605039-VERI-1605089).
- Secure Computing; internet security; Just How Critical is Data Integrity?; vol. 1, No. 1; Feb. 1997; Secure Computing Corporation; (VERI-1605627-VERI-1605630).
- Secure Computing; Internet Security; Payne, Data; Elvis spotted?; vol. 1, No. 2, Mar. 1997; Secure Computing Corporation; (VERI-1605631-VERI-1605634).
- Secure Computing; internet security; Victimized company learns hard lesson; vol. 1, No. 3, Apr. 1997; Secure Computing Corporation; (VERI-1605623-VERI-1605626).
- Secure Computing; Lockout™ DES; Client software; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605766-VERI-1605767).
- Secure Computing; Lockout™ DES; Identification and authentication; 1995; Secure Computing Corporation; (VERI-1605772-VERI-1605773).
- Secure Computing; Lockout™ DES; Lockout™ login agent and authentication server; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605768-VERI-1605769).
- Secure Computing; LOCKOut™ FORTEZZA; Strong identification and authentication; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605770-VERI-1605771).
- Secure Computing; LOCKOut™ Identification and Authentication; Nov. 8, 1996; Secure Computing Corporation; (VERI-1605606-VERI-1605607).
- Secure Computing; Press Release; Secure Computing Announces Immediate Availability of Sidewinder 3.0; Security Server Employs Fully Integrated Perimeter Security, IPsec Interoperable Encryption, Strong User Authentication, and E-mail Content Filtering; St. Paul, Minn.; Sep. 17, 1996; Secure Computing Corporation; (VERI-1606154-VERI-1606155).
- Secure Computing; Secure Computing Demonstration Software; Check out our demos for LOCKOut™ and Sidewinder™; Secure Computing Corporation; Nov. 1995; (VERI-1606130).
- Secure Computing; Sidewinder™ Security Server; Apr. 1997; Secure Computing Corporation; (VERI-1606152-VERI-1606153).
- Secure Computing; SNS Deployments; Mar. 1997; Secure Computing Corporation; (VERI-1606175).
- Secure Computing; SNS MLS Solution Set; Mar. 1997; Secure Computing Corporation; (VERI-1606176-VERI-1606177).
- Secure Computing; SNS Product Evolution; Mar. 1997; Secure Computing Corporation; (VERI-1606178-VERI-1606179).
- Secure Computing; SNS support and training services, World class; Secure Computing Corporation offers a variety of LOCK® Secure Network Server Installation, Training, and Maintenance programs; Nov. 1996; (VERI-1606103-VERI-1606106).
- Secure Computing; What's New?; Secure Computing Corporation; Feb. 1997; (VERI-1606156-VERI-1606157).
- Security Dynamics, Inc.; Kerberos and 3<sup>rd</sup> Party Authentication; Version 2.1; Mar. 1994; 7 pages.
- Security.itworld.com; Curing Remote-Access Security Ailments; Jan. 1996; 5 pages.
- SET Secure Electronic Transaction Specification; Book 1: Business Description; Version 1.0; May 31, 1997; 80 pages.
- SET Secure Electronic Transaction Specification; Book 3: Formal Protocol Definition; Version 1.0; May 31, 1997; 251 pages.
- SET Secure Electronic Transactions Website Archive; <http://web.archive.org/web/19981206111521/http://www.setco.org/>; Dec. 6, 1998; 1 page.
- SET; External Interface Guide to SET Secure Electronic Transaction; Sep. 24, 1997; 118 pages.
- Siau, K.; Xcert Software, Inc.; To appear in Journal of Information Technology; Nov. 1998; 26 pages.
- Siebenlist, et al.; RFC 68.4—DCE v.r.m Public Key Certificate Login—Functional Specification; Apr. 1998; 20 pages.
- Simpson, W.; RFC 1661—The Point-to-Point Protocol (PPP); Jul. 1994; 50 pages.

- Simpson, W.; RFC 1994—PPP Challenge Handshake Authentication Protocol (CHAP); Aug. 1996; 13 pages.
- Smith, Sean; Secure Coprocessing Applications and Research Issues; Computer Research and Applications Group (CIC-3); Los Alamos National Laboratory; Los Alamos Unclassified Release LA-UR-96-2805; Aug. 1, 1996; (VERI-1606131-VERI-1606147).
- St. Johns, M.; RFC 912—Authentication Service; Sep. 1984; 3 pages.
- St. Johns, M.; RFC 931—Authentication Server; Jan. 1985; 5 pages.
- Stallings, W.; Mecklermedia's Official Internet World™ Internet Security Handbook; Sep. 1995; 20 pages.
- Stefik, M.; Internet Dreams—Archetypes, Myths, and Metaphors; 1996; 2 cover pages and pp. 219-253 ("Letting Loose the Light: Igniting Commerce in Electronic Publication").
- Stefik, M.; Trusted Systems—Devices that enforce machine-readable rights to use the work of a musician or author may create secure ways to publish over the Internet; Scientific American; Mar. 1997; pp. 78-81.
- Stevens, W. Richard; "TCP/IP Illustrated: the protocols;" vol. 1; May 1994; cover page and pp. 33-39.
- Stronghold; Community ConneXion announces Stronghold version 1.2; Released: Jul. 16, 1996; Red Hat, Inc.; (CA956558-CA956559).
- Stronghold; XCert announces co-marketing agreement to reach largest Internet server market; Released: May 13, 1996, Red Hat, Inc.; (CA956560-CA956561).
- The Open Group; DCE, Distributing Computing Environment Overview; 1996; 7 pages.
- The Open Group; DCE, Distributing Computing Environment, DCE Glossary of Technical Terms; 1996; 4 pages.
- The Open Group; DCE, Distributing Computing Environment, OSF DCE 1.2.2 New Features; 1996; 5 pages.
- The Open Group; Draft Technical Standard, DCE 1.2.3 Public Key Certificate Login (Draft 0.8 for Company Review); Aug. 1998; 52 pages.
- The Open Group; Presentation at the Open Group Member's Meeting re DCE RFC 68.4 Public Key Certificate-Based DCE Login; Apr. 1998; 24 pages.
- The Open Group; Press Release: The Open Group and The Securities Industry Middleware Council Announce Security Solution for Wall Street—*Integrating Smart Cards and DCE*; Jun. 1998; 3 pages.
- The Open Group; Technical Standard DCE 1.1; Authentication and Security Services; Aug. 1997; 100 pages.
- The Open Group, The Open Group Announces General Availability of DCE 1.2.2 with Security and File System Enhancements; Dec. 1996; 6 pages.
- TIS; Defense Department Chooses Trusted Information Systems to Provide Network Firewall Plus E-Mail Security; Trusted Information Systems, Inc.; Jul. 10, 1996; (CA955278-CA995279).
- TIS; Firewall Product Functional Summary; NCSA (National Computer Security Association); Trusted Information Systems, Inc.; Jul. 22, 1996; (CA955280-CA955299).
- TIS; Firewall User's Overview; Trusted Information Systems, Inc.; Version dated Feb. 8, 1994; (CA955486-CA955490).
- TIS; Installing the Trusted Information Systems Internet Firewall Toolkit; Marcus J. Ranum; 1997; (CA955300-CA955347).
- TIS; Major Enhancements to Industry-Leading Gauntlet™ Internet Firewall; Trusted Information Systems, Inc.; Jul. 22, 1996; (CA955412-CA955414).
- TIS; Marcus J. Ranum et al.; A Toolkit and Methods for Internet Firewalls; Trusted Information Systems, Inc.; (CA955478-CA955485) 1997.
- TIS; TIS Firewall Toolkit: Configuration and Administration; Trusted Information Systems, Inc.; Version dated Feb. 17, 1994; (CA955264-CA955277).
- TIS; TIS Firewall Toolkit: Overview, Trusted Information Systems, Inc.; Version dated Jun. 30, 1994; (CA955398-CA955411).
- TIS; TIS Firewall Toolkit; Information Systems, Inc.; Sep. 1996; (CA955348-CA955397).
- TIS; Trusted Information Systems Enhances Industry-Leading Gauntlet™ Internet Firewall; Trusted Information Systems, Inc.; Jan. 23, 1996; (CA955415-CA955417).
- TIS; Trusted Information Systems extends security throughout the network with additions to Gauntlet™ Internet Firewall; Trusted Information Systems, Inc.; Apr. 2, 1996; (CA955418-CA955420).
- TIS; Trusted Information Systems Internet Firewall Toolkit: An Overview; Trusted Information Systems, Inc.; 1993; (CA955421-CA955477).
- Tom Sheldon's Linktionary; FORTEZZA Linktionary entry; Aug. 29, 2006; 2 pages.
- Tung; The Moron's Guide to Kerberos, Version 1.2.2; Dec. 1996; 11 pages.
- Tuvell, W.; RFC 98.0—Challenges Concerning Public-Key in DCE; Dec. 1996; 48 pages.
- U.S. Department of Commerce/National Institute of Standards and Technology, FIPS PUB 196—Entity Authentication Using Public Key Cryptography; Feb. 1997; 52 pages.
- U.S. Department of Commerce; Federal Information Processing Standards Publication 83: Specification for Guideline on User Authentication Techniques for Computer Network Access Control; 1980; 41 pages.
- U.S. Government; Demonstration Plan for JWID 97; Feb. 1997; 20 pages.
- Udell, Jon; Server and client certificates aren't yet widely used for authentication; but that's changing fast. Here's a progress report, Web Project; Digital IDs; Mar. 19, 1997; (CA956461-CA956468).
- Vollbrecht, J., et al.: AAA Authorization Application Examples; Request for Comments: 2905; Aug. 2000; 53 pages.
- Vollbrecht, J., et al.: AAA Authorization Framework; Request for Comments: 2904; Aug. 2000; 36 pages.
- V-One; "V-One Announces SmartWall DMS (TM)" Release DMS/Symposium & Demonstration/V-One Information; V-One Corporation; Dec. 4, 1996; (CA955694-CA955696).
- V-One; Archived News Articles; V-One Corporation; (CA955730-CA955732), 1997.
- V-One; Brian Santo; V-One Raises SmartGATE ; (Reprinted from Electronic Engineering Times, Dec. 11, 1995); V-One Corporation; (CA956273-CA956275).
- V-One; CSI Firewall Matrix Search Results; SmartWALL; V-One Corporation; (CA955580-CA955581), 1996.
- V-One; Form S-1/A; V-One CORP/DE-VONE, Filed Sep. 6, 1996, Amended Registration statement for face-amount certificate companies; (CA956332-CA956449).
- V-One; Form S-1; V-One CORP/DE-VONE, Filed Jun. 21, 1996, General form of registration statement: Initial statement; (CA955843-CA956272).
- V-One; Former Spyglass Vice President Joins V-One; V-One Corporation; 1996; (CA955722-CA955723).
- V-One; General Electric Information Services Teams with V-One in New Secure Internet Offering; First Deployment of V-One's SmartGATE Enables the World's Only Smart Card Solution on the Internet; (Reprinted from Business Wire, Feb. 9, 1996); V-One Corporation; (CA955574-CA955576).
- V-One; HPbler Erick; CyberWallet Offered as Secure Way to Conduct Share Trading On-Line; (Reprinted from Securities Industry Daily, Internet Technology, vol. VII, No. 190, Sep. 29, 1995); V-One Corporation; (CA957599-CA957601).
- V-One; Internet Firewalls Frequently Asked Questions; V-One Corporation; Marcus J. Ranum; 1995; (CA955632-CA955643).
- V-One; Karen Rodriguez; New Gateway Verifies Secure Server Link; (Reprinted from Communications Week, Dec. 11, 1995); V-One Corporation; (CA955681-CA955682).
- V-One; Marcus J. Ranum; Electronic Commerce and Security, V-One Corporation; (CA955598-CA955604), 1996.
- V-One; Marcus Ranum, Father of Firewall Joins V-One as Chief Scientist; V-One Corporation; Oct. 1996; (CA955728-CA955729).
- V-One; Marcus Ranum; V-One's Security Middleware Product Suite; V-One Corporation; (CA956452-CA956458).
- V-One; Marjanovic, Steven; Software Beef up Security of Internet Transactions; (Reprinted from American Banker(R), The Daily Financial Services Newspaper, Friday, Feb. 16, 1996, p. 13); V-One Corporation; (CA955551-CA955553).
- V-One; MCI and V-One Corporation Announce Sales Alliance Agreement; V-One Corporation; Jan. 27, 1997; (CA955714-CA955716).

V-One; New and Noteworthy: A rundown of recent electronic commerce products and services; (Reprinted from ComputerWorld, Feb. 5, 1996, vol. 30, No. 6); V-One Corporation; (CA95578-955579).

V-One; New Network Security Products Spur On-line Interest; (Reprinted from Electronic Commerce News (PBI), Mar. 11, 1996); V-One Corporation; (CA955644-CA955647).

V-One; Nick Wingfield; V-One promises net security: SmartGATE client/Server tool encrypts across TCP/IP, (Reprinted from InfoWorld, Internet, Dec. 11, 1995); V-One Corporation; CA955630-CA955631).

V-One; NSA Chooses V-One to Protect DMS Networks; (Reprinted from Government Computer News, The National Newspaper of Government Computing, vol. 15, No. 8, Apr. 15, 1996); V-One Corporation; (CA955626).

V-One; Paul Merenbloom; SmartGate Internet Security gives good name to middleware: Lan Talk, (Reprinted from InfoWorld, Feb. 19, 1996); V-One Corporation; (CA955627-CA955629).

V-One; Resellers and Distributors; V-One Corporation; (CA955816-CA955820), 1997.

V-One; Reva Basch; SmartWall Easing Internet Security Concerns; (Reprinted from PC Today, Feb. 1996, p. 34); V-One Corporation; (CA955683-CA955685).

V-One; Security Middleware; Beyond Firewalls; V-One Corporation; Revised: May 23, 1996; (CA955746-CA955747).

V-One; Smartgate: Making networks safe for business. Administrator's Guide; V-One Corporation; 1998; (CA957127-CA957460).

V-One; SmartGATE; Secure Connectivity over an Untrusted Network; V-One Corporation; Jan. 15, 1996; (CA955810-0A955815).

V-One; SmartGATE™ A product of Security Middleware; V-One Corporation; 1996; (CA956276-CA956277).

V-One; SmartWall(TM) to Augment Defense Messaging System: Protecting Highest Military Network; V-One Corporation; 1996; (CA955697-CA955698).

V-One; SmartWall(TM) to Augment Defense Messaging System: Protecting Highest Military Network; V-One Corporation; 1996; (CA955699-CA955700).

V-One; Success Stories: Regional Law Enforcement Network Reduces Violent Crime While Saving Time and Money; Customer Case Study: Regional Law Enforcement Network; V-One Corporation; (CA956329-CA956331), 1996-1997.

V-One; The Internet Just Got Real!; Marketing Strategy and Mission; V-One Corporation; (CA955549-CA955550), 1996.

V-One; Trusted Information Systems (TIS) Supports V-One's Security Middleware Product SmartGate(TM); TIS to Support SmartGATE Technology in Gauntlet Product Family; V-One Corporation; May 1996; (CA955718-CA955721).

V-One; V-One Announces Business Alliance With Lockheed Martin Federal Systems in Gaithersburg; V-One Corporation; Oct. 31, 1996; (CA955688-CA955690).

V-One; V-One Announces SmartGate; Enabling Open and Secure Business Transactions on the Internet; New Class of Security Product Allows Businesses to Build a secure Transaction Environment with Existing Legacy or New Client/Server Applications; V-One Corporation; Dec. 11, 1995; (CA955691-CA955693).

V-One; V-One Announces SmartGate; Enabling Open and Secure Business Transactions on the Internet; New Class of Security Product Allows Businesses to Build a Secure Transaction Environment with Existing Legacy or New Client/Server Applications; V-One Corporation; Dec. 1996; (CA955701-CA955703).

V-One; V-One Announces SmartWall DMS(TM); V-One Corporation; Oct. 25, 1996; (CA956686-CA955687).

V-One; V-One Chisels Commerce Drawbridge in Internet Firewalls; (Reprinted from Network Computing, Jan. 15, 1996); V-One Corporation; 1 page.

V-One; V-One Corporation Defines a New Class of Security Products: Security Middleware; Industry's First Security Middleware product, SmartGATE, will be demonstrated at RSA Conference in San Francisco; V-One Corporation; Jan. 1996; (CA955710-CA955713).

V-One; V-One launches smart card at FSU; (Reprinted from Online Banking newsletter, Market intelligence for banking executives, vol. I, Issue 8, Mar. 11, 1996); V-One Corporation; CA955717).

V-One; V-One Security for a Connected World; V-One Corporation; prior to Aug. 29, 2002; (CA955491-CA955546).

V-One; V-One SmartWall is Best in Infosecurity News Security Supplement; V-One Corporation; Oct. 1996; (CA955726-CA955727).

V-One; V-One to Secure Oracle's Database Network Products; V-One Corporation; Oct. 1996; (CA955724-CA955725).

V-One; V-One; Leader in Providing Internet Security, Expands Reach Through Agreements with 14 Resellers; VARs Cite Hot Market and Corporate Need for Secure Transactions Via Internet; V-One Corporation; Sep. 9, 1996; (CA957602-CA957604).

V-One; V-One, Security Dynamics Announce Technological Interoperability; Security Dynamics' Leading SecurID Authentication Compatible with V-One's Top-Ranked Firewall, SmartWall; V-One Corporation; Feb. 1996; (CA955704-CA955706).

V-One; V-One; Software.com, and VNI Partner to Offer First-Of-Its-Kind Secure Messaging; Sender Authentication and Guaranteed Delivery Now Possible Through Post Office(TM) with SmartGATE(TM); V-One Corporation; Apr. 1996; (CA957595-CA957598).

V-One; V-One's Executive Team; V-One Corporation; 1996; (CA956450-CA956451).

V-One; VPN Authentication Encryption Access Control; Van Short, V-One Corporation; (CA955765-CA955809), 2000.

V-One; VPN Deployment Lessons Learned; Van Short, V-One Corporation; prior to Aug. 29, 2002; (CA955748-CA955764).

Wagner, Mitch; Vanguard makes net link with clients (Reprinted from Computer World, vol. 30, No. 8, Feb. 19, 1996); (CA957461-CA957462).

Wallace, B.; RADIUS to secure remote access; Apr. 1995; 3 pages.

Warner, M.; RFC 85.0—Improved Public Key Login Protocols for DCE; Oct. 1995; 17 pages.

Weiner, Bruce; "Netegrity SiteMinder 4.61 with Microsoft Active Directory AuthMark Performance;" Apr. 18, 2002; 4 pages.

Westlaw; (Anonymous); Open Market to acquire Folio Corporation; Information Today; Apr. 1997; ProQuest Info&Learning; (VERI-1605301-VERI-1605302).

Westlaw; (Anonymous); Open Market unleashes new class of Web software; Information Today; Apr. 1996; ProQuest Info&Learning (VERI-1605199-VERI-1605202).

Westlaw; (Anonymous); Retail technology online; Chain Store Age; May 1996; ProQuest Info&Learning; (VERI-1605196-VERI-1605198).

Westlaw; (Anonymous); Web sheet; Manufacturing Systems; Aug. 1997; ProQuest Info&Learning; (VERI-1605276).

Westlaw; [Compilation of various articles]; (VERI-1603872-VERI-1603900), 1993-1996.

Westlaw; Adams, Charlotte; Security applications drive government sales (smart cards); Federal Computer Week; Sep. 19, 1994; vol. 8; Issue 28; (VERI-1606804).

Westlaw; Barnes, Angela; Section: Report on Business; Dow drops 44.83, but Nasdaq raises to record Wall Street puzzled by jobs report; Globe and Mail; Sep. 6, 1997; (VERI-1606833-VERI-1606834).

Westlaw; Block, Valerie; Florida State U. Smartening Up Its Student IDs; American Banker; Mar. 12, 1996, vol. 161; Issue 48; (VERI-1606762-VERI-1606763).

Westlaw; Bowen, Ted Smalley; Powersoft hones Internet tool strategy; InfoWorld; Aug. 26, 1996; ProQuest Info & Learning; (VERI-1605184-VERI-1605185).

Westlaw; Bucholtz, Chris; E-entrepreneurs make their mark; Telephony, Internet Edge Supplement; Oct. 6, 1997; ProQuest Info & Learning; (VERI-1605256-VERI-1605259).

Westlaw; Card Briefs: On-Line Security Eyed for Florida St. ID Tool; American Banker; Jun. 17, 1996; vol. 161; Issue 115; (VERI-1606752).

Westlaw; Carr, Jim; Users wade through electronic-commerce market; InfoWorld; Jun. 23, 1997; ProQuest Info&Learning (VERI-1605292-VERI-1605296).

Westlaw; Chrysalis-ITS Introduces LunaCA; Cryptography System Adds Trust and Assurance to PKI Certification Authority; Sinocast; Nov. 10, 1997; (VERI-1606829-VERI-1606830).

Westlaw; Cox, John; Cadis brings organization to the Web; Network World; Feb. 10, 1997; ProQuest Info&Learning; (VERI-1605310-VERI-1605311).

Westlaw; Damore, Kelley; Hardware makers hit the market with server bundles; Computer Reseller News; May 13, 1996; ProQuest Info&Learning; (VERI-1605194-VERI-1605195).

Westlaw; Darrow, Barbara; Web produces product storm; Computer Reseller News; Dec. 9, 1996; ProQuest Info&Learning (VERI-1605164-VERI-1605166).

Westlaw; Davis, Beth; Review Set for Secure Directory Access Spec; TechWebNews; Apr. 7, 1997; (VERI-1606866).

Westlaw; Davis, Jessica; Novell commerce server slides; InfoWorld; Jul. 8, 1996; ProQuest Info&Learning (VERI-1605189-VERI-1605190).

Westlaw; Dunlap, Charlotte; Open Market inks alliance with Portland Software; Computer Reseller News; Aug. 18, 1997; ProQuest Info&Learning (VERI-1605283-VERI-1605284).

Westlaw; Dunlap, Charlotte; Open Market woos Web Integrators; Computer Reseller News; Aug. 5, 1996; ProQuest Info&Learning (VERI-1605186-VERI-1605187).

Westlaw; Edwards, Morris; The electronic commerce juggernaut; Communications News; Sep. 1997; ProQuest Info&Learning. (VERI-1605262-VERI-1605265).

Westlaw; Engler, Natalie; The second coming of electronic commerce; Computerworld; Dec. 15, 1997; ProQuest Info&Learning (VERI-1605229-VERI-1605234).

Westlaw; Erlanger, Leon; Disarming the Net (security challenges resulting from connection to the Internet) (Network Edition) (Internet/Web/Online Service Information); PC Magazine; Jun. 10, 1997; vol. 16; Issue 11; (VERI-1606856-VERI-1606861).

Westlaw; Extruded tubing wall thickness; Modern Plastics; May 1986; (VERI-1606812).

Westlaw, Frank, Diane; The new ROI in point of sale; Datamation; The Gale Group; (VERI-1605776), Nov. 1997.

Westlaw; French Payment Developer Puts Banks in the Hot Seat; Bank Technology News; May 1, 1997; (VERI-1606862-VERI-1606864).

Westlaw; Fulcher, Jim; Shopping made easy; Manufacturing Systems; Oct. 1997; ProQuest Info&Learning; (VERI-1605238-VERI-1605239).

Westlaw; GEIS Using V-One SmartGATE; Report on Electronic Commerce; Feb. 20, 1996; vol. 3; Issue 4; (VERI-1606764).

Westlaw; Gengler, Barbara; V-One, Rockville, Md. (SmartGATE secure transaction technology for client/server applications) (Product Information) (Brief Article); Internetwork; vol. 7; Issue 4; (VERI-1606760), Apr. 1996.

Westlaw; Guenette David R.; Enterprising information; EMedia Professional; Nov. 1997; ProQuest Info&Learning. (VERI-1605240-VERI-1605251).

Westlaw; Harrison, Ann; Reach out and buy something; Software Magazine; Apr. 1997; ProQuest Info&Learning; (VERI-1605305-VERI-1605309).

Westlaw; Hudgins-Bonafield, Christy; Bridging the Business-to-Business Authentication Gap; Network Computing; Jul. 1997.

Westlaw; Hudgins-Bonafield, Christy; Mapping the Rocky Road to Authentication; Network Computing; Jul. 15, 1997; (VERI-1606837-VERI-1606839).

Westlaw; Hummingbird Does New Java Deal; Newsbytes PM; Sep. 5, 1997; (VERI-1606835).

Westlaw; Hummingbird Gets Secure Java; ENT, Sep. 24, 1997; (VERI-1606831).

Westlaw; Humphrey, John H., et al.; Comparison tests streamline complex dial-up modem measurements and spring some surprises; Electronic Design; May 1987; vol. 35; (VERI-1606807-VERI-1606811).

Westlaw; Internet Security & Privacy: V-One and Software.com Provide Secure Messaging; Internet Content Report; Jun. 1, 1996; vol. 1; Issue 6; (VERI-1606755).

Westlaw; Items of Interest; Report on Smart Cards; May 6, 1996; vol. 10; Issue 9; (VERI-1606758-VERI-1606759).

Westlaw; Java security technology licensed from Xcert Software; Canada StockWatch; Sep. 4, 1997; (VERI-1606836).

Westlaw; Jones, Chris; iCat and Cadis link online database to Web; InfoWorld; Feb. 10, 1997; ProQuest Info&Learning (VERI-1605312-VERI-1605313).

Westlaw; Jones, Chris; OM-Transact connects to invoice and ordering systems; Infoworld; Dec. 9, 1996; ProQuest Info&Learning (VERI-1605174-VERI-1605175).

Westlaw; Jones, Chris; Selling online; InfoWorld; Mar. 17, 1997; ProQuest Info&Learning; (VERI-1605274-VERI-1605275).

Westlaw; Jones, Chris; SGI will soon deliver virtual-store tools; InfoWorld; Dec. 23-30, 1996; ProQuest Info&Learning; (VERI-1605167-VERI-1605168).

Westlaw; Jones, Chris; Vendors back SET protocol with product announcements; InfoWorld; Feb. 3, 1997; ProQuest Info&Learning (VERI-1605314-VERI-1605315).

Westlaw; Key Management System; Entrust; Network Computing; May 1, 1997; (VERI-1606865).

Westlav; Kohlhepp, Robert J.; Securing Intranet Data With SSL Client Certificates; Network Computing; Jul. 1, 1997; (VERI-1606852-VERI-1606855).

Westlaw; Krill, Paul; Novell to adopt Java, ActiveX architectures; InfoWorld; Mar. 25, 1996; ProQuest Info&Learning (VERI-1605208-VERI-1605210).

Westlaw; Kruger, Peter; The net takes its toll; Communications International; May 1996; ProQuest Info&Learning (VERI-1605191-VERI-1605193).

Westlaw; Kutler, Jeffrey; Vendors Ready—and Waiting—for E-commerce; American Banker; Feb. 2, 1996; vol. 161; Issue 22; (VERI-1606767-VERI-1606769).

Westlaw; Lawton, George; Surf's up! The Internet is here. (part 1) (includes related article); Telephony; Jul. 17, 1995; vol. 229; Issue 3; (VERI-1606788-VERI-1606793).

Westlaw; Lewis, Peter H.; Internet Commerce: Hold the Anchovies; New York Times; Apr. 7, 1995; (VERI-1606800-VERI-1606801).

Westlaw; Making Net Management Easier; Sinocast; Dec. 22, 1997; (VERI-1606827-VERI-1606828).

Westlaw; Masud, Sam; iCat signs 120 VARs, Ingram Micro; Computer Reseller News; Jan. 13, 1997; ProQuest Info&Learning (VERI-1605316-VERI-1605317).

Westlaw; Masud, Sam; OpenMarket hopes to cash in on electronic commerce; Computer Reseller News; Oct. 28, 1996; ProQuest Info&Learning; (VERI-1605178-VERI-1605179).

Westlaw; Messmer, Ellen, et al.; Holiday networking extravaganza on tap; Network World; Dec. 9, 1996; ProQuest Info&Learning (VERI-1605160-VERI-1605163).

Westlaw; Messmer, Ellen; Open Market software separates Web content, transaction management; Network World; Mar. 11, 1996; ProQuest Info&Learning (VERI-1605206-VERI-1605207).

Westlaw; Messmer, Ellen; Start-up's service dodges Net sales tax; Network World; Jun. 30, 1997; ProQuest Info&Learning (VERI-1605297-VERI-1605298).

Westlaw; Michel, Roberto; The Net benefits; Manufacturing Systems; Feb. 1997; ProQuest Info&Learning (VERI-1605277-VERI-1605282).

Westlaw; Millman, Howard; Profit ploys for increased income; InfoWorld; Nov. 3, 1997; ProQuest Info&Learning (VERI-1605235-VERI-1605237).

Westlaw; Mohan, Suruchi; Effective Internet commerce to hinge on directories; InfoWorld; Sep. 8, 1997; ProQuest Info&Learning; (VERI-1605266-VERI-1605270).

Westlaw; Murphy, Brian; Telecommunications talk; magazines online, new bulletin boards, and new products; Creative Computing; Jan. 1985; vol. 11; (VERI-1606813-VERI-1606816).

Westlaw; Nash, Kim S.; Open Market aids Web site upkeep; Computerworld; Mar. 11, 1996; ProQuest Info&Learning (VERI-1605211-VERI-1605212).

Westlaw; New Products; Defense Daily; Sep. 15, 1997; vol. 2; (VERI-1606832).

Westlaw; New Security Technology Products; Security Technology News; Aug. 26, 1994; vol. 2; Issue 17; (VERI-1606805).

- Westlaw; Newing, Rod; A new computing architecture is coming; Management Accounting-London; Dec. 1996; ProQuest Info&Learning (VERI-1605169-VERI-1605173).
- Westlaw; Online; Report on Electronic Commerce; Apr. 30, 1996; vol. 3; Issue 9; (VERI-1606876-VERI-1606877).
- Westlaw; Orenstein, Alison F.; Banks help merchants tap Internet 'sales floor'; Bank Systems & Technology; Apr. 1997; ProQuest Info&Learning (VERI-1605303-VERI-1605304).
- Westlaw; Ostertag, Krista; Tightening the Web, fixing the holes; Varbusness; Apr. 1, 1996; (VERI-1606761).
- Westlaw; Pappalardo, Denise; ISPs dress up Web hosting services; Network World; Jul. 28, 1997; ProQuest Info&Learning; (VERI-1605290-VERI-1605291).
- Westlaw; Personnel Roundup; Newsbytes PM; Oct. 13, 1995; (VERI-1606783-VERI-1606784).
- Westlaw; Poole, Jackie; Commerce-enabled sites from ANS; InfoWorld; Jul. 21, 1997; ProQuest Info&Learning (VERI-1605288-VERI-1605289).
- Westlaw; Premenos and Open Market Announce Strategic OEM Alliance; PR Newswire, Mar. 4, 1996; The Gale Group; (VERI-1605774-VERI-1605775).
- Westlaw; Prince, Cheryl J.; Building an Internet payments franchise; Bank Systems & Technology; Sep. 1996; ProQuest Info&Learning (VERI-1605182-VERI-1605183).
- Westlaw; Reuters, Jennifer Genevieve; Section: Business; IPOS Looked Golden in '95; Memphis Commercial Appeal; Memphis, TN; Jan. 2, 1996; (VERI-1606771-VERI-1606772).
- Westlaw; Reuters; Section: Business; Tech Talk; St. Louis Post-Dispatch; Dec. 13, 1995; (VERI-1606773).
- Westlaw; Rodriguez, Karen; Open market targets business; CommunicationsWeek; Mar. 11, 1996; ProQuest Info&Learning (VERI-1605203).
- Westlaw; Schmidt, Karen; Section: Metro Hartford; Putting a High-Tech Spin on Computer-Aided Design in Newington; Hartford Courant; Sep. 21, 1995; (VERI-1605785-VERI-1606786).
- Westlaw; Section: Business; ACME Sets Agreement to Market Power Unit; Buffalo News; Feb. 22, 1993; (VERI-1606806).
- Westlaw; Section: Business; Financing Deal; Hartford Courant; Aug. 26, 1995; (VERI-1606787).
- Westlaw; Section: Financial; BioWhittaker Posts 62% Gain in Profits for 4<sup>th</sup> Quarter; Baltimore Sun; Dec. 12, 1995; (VERI-1606774-VERI-1606776).
- Westlaw; Section: Financial; MD. Software Product Offers Internet Security; Baltimore Sun; Dec. 9, 1995; (VERI-1606779).
- Westlaw; Section: Financial; Phone Users Can Join in Testing a Speedier Data-Send Service; Baltimore Sun; Oct. 31, 1996 (VERI-1606780-VERI-1606782).
- Westlaw; Spyglass offers software tailoring Mosaic for use by business on the Internet; Software Industry Report; Dec. 19, 1994; vol. 26; Issue 24; (VERI-1606802-VERI-1606803).
- Westlaw; Symoens, Jeff; Integration is key to Commerce; InfoWorld; Oct. 13, 1997; ProQuest Info&Learning (VERI-1605254-VERI-1605255).
- Westlaw; Symoens, Jeff; Transact 3.0: Scalable solution; InfoWorld; Sep. 8, 1997; ProQuest Info&Learning, (VERI-1605271-VERI-1605273).
- Westlaw; Technology; Crackdown on Internet security; Financial Times Mandate; May 30, 1996; (VERI-1606756).
- Westlaw; UK-London; computerized human resource information system (With participation by GATT countries); Tenders Electronic Daily; Jul. 14, 1995; (VERI-1606795-VERI-1606797).
- Westlaw; VeriSign Announces New Partners; Report on Smart Cards; May 6, 1996, vol. 10; Issue 9; (VERI-1606757).
- Westlaw; Virtual Open Network Environment Corp.; Going Public the IPO Reporter; Aug. 19, 1996; vol. 20; issue 34; Securities Data Publishing; (VERI-1606750-VERI-1606751).
- Westlaw; V-One Securing Payments with Enhanced Firewalls; Retail Delivery News; Jun. 7, 1996; vol. 1; Issue 12; (VERI-1606753-VERI-1606754).
- Westlaw; Wagner, Mitch; Open Market upgrade will support big business on 'net; Computerworld; Dec. 9, 1996; ProQuest Info&Learning (VERI-1605176-VERI-1605177).
- Westlaw; Wagner, Mitch; Start-up will outsource 'net transactions; Computerworld; Jun. 30, 1997; ProQuest Info&Learning (VERI-1605299-VERI-1605300).
- Westlaw; Walsh, Jeff; Open Market announces SiteDirector 4.1; InfoWorld; Dec. 15, 1997; ProQuest Info&Learning (VERI-1605227-VERI-1605228).
- Westlaw; Wexler, Joanie; AT&T rounds out E-commerce line; Network World; Oct. 14, 1996; ProQuest Info&Learning (VERI-1605180-VERI-1605181).
- Westlaw; Who's who in the CA market; Network Computing; Jul. 15, 1997; (VERI-1606850-VERI-1606851).
- Westlaw; Wilder, Clinton, et al.; Pushing outside the enterprise; Informationweek; Aug. 4, 1997; ProQuest Info&Learning (VERI-1605285-VERI-1605287).
- Westlaw; Wilder, Clinton, et al.; Trusting the Net; Informationweek; Oct. 14, 1996; ProQuest Info&Learning (VERI-1605156-VERI-1605159).
- Westlaw; Wilder, Clinton; Distributors get their own shot at Web sales; Informationweek; Sep. 8, 1997; ProQuest Info&Learning (VERI-1605260-VERI-1605261).
- Westlaw; Wilder, Clinton; E-commerce gets real; Informationweek; Dec. 9, 1996; ProQuest Info&Learning (VERI-1605153-VERI-1605155).
- Westlaw; Wilder, Clinton; E-commerce hosting services to expand; Informationweek; Jul. 22, 1996; ProQuest Info&Learning (VERI-1605188).
- Westlaw; Wilder, Clinton; Focus on e-commerce; Informationweek; Oct. 6, 1997; ProQuest Info&Learning (VERI-1605252-VERI-1605253).
- Westlaw; Willett, Shawn; Novell to license Java, build online tools; Computer Reseller News; Mar. 18, 1996; ProQuest Info&Learning (VERI-1605204-VERI-1605205).
- Westlaw; Wilson, Donald C.; Highest and best use: Preservation use of environmentally significant real estate; Appraisal Journal; Jan. 1996; ProQuest Info&Learning (VERI-1605214-VERI-1605226).
- Westlaw; Wilson, Donald C.; The principle of rank substitution; Appraisal Journal; Jan. 1997; ProQuest Info&Learning (VERI-1605318-VERI-160531).
- Willens, S., et al.; "Remote Authentication Dial in User Service (RADIUS) draft-ietf-nasreq-radius-01.txt (c); May 1994; pp. i, ii, and 1-35.
- Wirbel, L.; Management platforms, virtual lans shine at show-NetWorld; gains aplenty; Electronic Engineering Times; Apr. 1996; 4 pages.
- Woo, Thomas Y.C., et al.; "Authentication for Distributed Systems;" to appear in Internet Besieged: Countering Cyberspace Scofflaws; 1997; 30 pages.
- Woo, Thomas Y.C., et al.; Authentication for Distributed Systems; Computer; Jan. 1992; pp. 39-52.
- Wood, B.; A Case for Avoiding Security-Enhanced HTTP Tools to Improve Security for Web-Based Applications; Feb. 1996; 7 pages.
- Workshop on Network and Distributed Systems Security; Krajewski, Jr., Marjan; Smart Card Augmentation of Kerberos; Feb. 1993; pp. 119-123.
- Workshop on Network and Distributed Systems; Dray, Jim, et al.; An Overview of the Advanced SmartCard Access Control System (ASACS); Feb. 1993; pp. 125-133.
- Workshop on Network and Distributed Systems; Schiller, Jeffrey I.; Issues Surrounding the Use of Cryptographic Algorithms and Smart Card Applications; Feb. 1993; cover page and pp. 115-118.
- Wu, Cheng C.; Remote Access Technology: Evaluating the Options; vol. 28, Issue 7; Jul. 1994; 7 pages.
- Xcert Software, Inc.; Excerpt from website; "Can You get through this door?"; 1996; 2 pages.
- Xcert; Fischer International Systems Corporation and Xcert Software Inc demonstrate the first web-based Certificate Authority to interoperate with hardware tokens; Xcert International Inc.; Nov. 12, 1996; (CA956555-CA956557).
- Xcert; Keng Siau, et al.; Xcert Software Inc.—The Next Step Forward (B); Aug. 1997; 7 pages.
- Xcert; Network Computing Magazine Names Xcert's Sentry CA as a 'Well-Connected' Award Nominee; Xcert International Inc.; Mar. 7, 1997; (CA956551-CA956552).

# US 8,387,155 B2

Page 17

Xcert; Sales FAQ (Frequently Asked Questions): Corporate and Product Overview; Xcert Software, Inc.; 1996-1997; (CA956507-CA956510).  
Xcert; Sales FAQ (Frequently Asked Questions): Download and Support; Xcert Software, Inc.; (CA956504-CA956506), 1997.  
Xcert; Sentry CA (Certificate Authority); Internet Security Technologies; Xcert International Inc.; 1997; (CA957605-CA957610).  
Xcert; Software Sentry News Media Backgrounder; Xcert International Inc.; Apr. 17, 1996; (CA956536-CA956538).  
Xcert; Software Sentry Technology Announcement; Xcert International Inc.; Apr. 18, 1996; (CA956539-CA956641).  
Xcert; The Xcert Sentry Access Control List Module; 1996; 3 pages.  
Xcert; Xcert Announces Co-Marketing Agreement to Reach Largest Internet Server Market; Xcert International Inc.; May 14, 1996; (CA956553-CA956654).  
Xcert; Xcert Software Announces Support for Litronic NetSign™; Xcert International Inc.; Jun. 11, 1997; (CA956545-CA956546).  
Xcert; Xcert Software Inc., Questions and Answers; 1996; 9 pages.  
Xcert; Xcert Software Inc., /html-docs; Xcert Software Inc.; 1996; (VERI-1605090).  
Xcert; Xcert Softwares is First to Demonstrate Certification Authority (CA) Interoperability; Xcert International Inc.; Mar. 21, 1997; (CA956550).  
Xcert; Xcert Software's Certification Authority and Access Control Technology Provides Privacy on Public Networks; Xcert International, Inc.; Jan. 27, 1997; (CA956542-CA956544).  
Xcert; Xcert Your Authority; Can You get through this door?; Xcert Software Inc.; 1996-1997; (CA957463-CA957464).  
Xcert; Xcert's New Certification Authority and Access Control Technology Offers Unprecedented Safeguards for Electronic Commerce and Communications; Xcert International Inc.; Jun. 24, 1996; (CA956547-CA956549).  
Xcert; XUDA Specification; Xcert Software, Inc.; (VERI-1605335-VERI-1605337), 1996.  
Xcert; XUDA: Xcert Universal Database API, Internet Security Technologies; Xcert International Inc.; (CA957616-CA957617), 1996.  
Yeong, et al.; RFC 1777—Lightweight Directory Access Protocol; Mar. 1995, 21 pages.  
Ylönen, T.; SSH—Secure Login Connections Over the Internet; Proceedings of the Sixth USENIX Security Symposium; Jul. 1996; 10 pages.  
Zborny, Michael R.; Securing Legacy TCP/IP Applications; Gartner, Inc.; ID No. SPA-AUZ-024; Dec. 28, 1995; (CA955741-CA955745).  
Zhong, Q.; Providing Secure Environments for Untrusted Network Applications; Proceedings of the 6<sup>th</sup> Workshop on Enabling Technologies Infrastructure for Collaborative Enterprises; 1997; pp. 277-283.  
Zisman, Alan; Local Software Products Helping to Blaze the Way to Secure Business Dealings on the Internet; Business in Vancouver; Issue 342; High Tech Office column; May 14, 1996; 2 pages.  
Zorn, G. et al.; "RADiUS Authentication Server MIB," Request for Comments: 2619; Jun. 1999; 16 pages.  
Menezes, A. et al.; "Handbook of Applied Cryptography;" CRC Press, Inc.; 1997; cover page and pp. 1-319, 321-383, 385-541, 543-661, and 663-780.  
Defendants' Opening Claim Construction Brief Regarding "Hardware Key" and "Access Key"; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 172; filed Jan. 28, 2011; 34 pages.  
Index of Evidence Supporting Defendants' Opening Claim Construction Brief Regarding "Hardware Key" and "Access Key"; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 173; filed Jan. 28, 2011; 451 pages.  
Plaintiff's Opening Claim Construction Brief Regarding "Hardware Key" and "Access Key"; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 178; filed Mar. 1, 2011; 24 pages.  
Index of Evidence Supporting Plaintiff's Opening Claim Construction Brief Regarding "Hardware Key" and "Access Key"; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 179; filed Mar. 1, 2011; 146 pages.  
Defendants' Reply Claim Construction Brief Regarding "Access Key" and "Hardware Key"; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 180; filed Mar. 21, 2011; 26 pages.  
Index of Evidence Supporting Defendants' Reply Claim Construction Brief Regarding "Hardware Key" and "Access Key"; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 181; filed Mar. 21, 2011; 41 pages.  
Transcript of Proceedings before the Honorable Lyle E. Strom United States Senior District Judge (Markman Hearing with Presentations); *Prism Technologies, LLC v. Adobe Systems Inc., et al.*, Case No. 8:10-cv-00220-LES-TDT; Doc. No. 226; hearings took place Apr. 11, 2011; 166 pages.  
Memorandum and Order (Markman); *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10CV220; Doc. No. 188; filed Jun. 1, 2011; 15 pages.  
Defendants' Opening Brief in Support of Motion for Summary Judgement of Noninfringement; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 289; filed Oct. 7, 2011; 30 pages.  
Plaintiff Prism Technologies, LLC's Opening Claim Construction Brief; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-00220-LES-TDT; Doc. No. 309; filed Oct. 17, 2011; 51 pages.  
Index of Evidence for Plaintiff Prism Technologies, LLC's Opening Claim Construction Brief; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-00220-LES-TDT; Doc. No. 310; filed Oct. 17, 2011; 356 pages.  
Adobe Systems Incorporated's Responses to Plaintiff Prism Technologies, LLC's Second Set of Interrogatories; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Nov. 3, 2011; 9 pages.  
Defendant Autodesk, Inc.'s Responses and Objections to Prism's Second Set of Interrogatories (Nos. 7-8); *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10-cv-220; dated Nov. 7, 2011; 7 pages.  
Defendants' Responsive Claim Construction Brief; *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Nov. 14, 2011; 63 pages.  
Index of Evidence in Support of Defendants' Responsive Claim Construction Brief; *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Nov. 14, 2011; 487 pages.  
Symantec Corporation's Objections and Responses to Prism Technologies LLC's Third Set of Interrogatories; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220-LES-TDT; dated Nov. 21, 2011; 9 pages.  
Memorandum and Order; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10CV220; dated Nov. 28, 2011; 10 pages.  
Plaintiff Prism Technologies, LLC's Reply Claim Construction Brief; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-00220-LES-TDT; Doc. No. 400; filed Dec. 2, 2011; 41 pages.  
Index of Evidence for Plaintiff Prism Technologies, LLC's Reply Claim Construction Brief; *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-00220-LES-TDT; Doc. No. 401; filed Dec. 2, 2011; 88 pages.  
Defendant National Instruments Corporation's Response to Plaintiff Prism Technologies, LLC's Third Set of Interrogatories; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Dec. 8, 2011; 7 pages.  
Defendant Adobe Systems Incorporated's First Supplemental Responses to Plaintiff Prism Technologies, LLC's Second Set of Interrogatories; (With Appendix A and Exhibits 1-48) *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Dec. 16, 2011; 1233 pages.  
Defendant National Instruments Corporation's First Supplemental Responses to Plaintiff Prism Technologies, LLC's Third Set of Interrogatories; *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Dec. 16, 2011; 8 pages.  
Symantec, Corporation's First Supplemental Objections and Responses to Prism Technologies LLC's Interrogatory Nos. 6 and 10;

- Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Dec. 16, 2011; 13 pages.
- Trend Micro Incorporated's Supplemental Objections and Responses to Prism's Second Set of Interrogatories (Nos. 7-8); *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Dec. 22, 2011; 1239 pages.
- McAfee, Inc.'s First Supplemental Response to Prism's Third Set of Interrogatories to McAfee, Inc. (Nos. 8-9); *Prism Technologies LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-CV-220-LES-TDT; dated Dec. 23, 2011; 1193 pages.
- Sage Software Inc.'s First Supplemental Responses to Plaintiff Prism Technologies, LLC's Third Set of Interrogatories; *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Dec. 23, 2011; 1237 pages.
- Defendant Autodesk, Inc.'s Supplemental Responses and Objections to Prism's Second Set of Interrogatories (No. 8); *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10-cv-220; dated Jan. 6, 2012; 1234 pages.
- Transcript of Proceedings Before the Honorable Lyle E. Strom United States Senior District Judge (Markman Hearing with presentations); *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10CV220; dated Jan. 12, 2012; 290 pages.
- Joint Stipulation on Claim Construction; *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10-cv-00220-LES-TDT; Doc. No. 440; dated Jan. 20, 2012; 11 pages.
- Memorandum and Order; *Prism Technologies, LLC v. Adobe Systems Incorporated, et al.*; Case No. 8:10CV220; Doc. No. 469; dated Feb. 14, 2012; 32 pages.
- Abadi et al.; "Authentication and Delegation with Smart-Cards;" Science of Computer Programming, 1993, pp. 91-113.
- Abraham, Dennis G., et al., "Transaction Security System," IBM Systems Journal, vol. 30, No. 2, 1991.
- Agha, Gul, et al., "Security and Fault-Tolerance in Distributed Systems: An Actor-Based Approach," Proceedings: Computer Security, Dependability; and Assurance: From Needs to Solutions, Jul. 7-9, 1998, pp. 72-88.
- Avolio, Frederick M., et al., "A Network Perimeter With Secure External Access," Jan. 25, 1994, pp. 1-11.
- Bertino, Elise, et al. "Protecting Information on the Web," Communications of the ACM, 2000, pp. 189-199.
- Bodoh, Dan, "Making the Most of the Internet for Failure Analysis," Proceedings from the 24th International Symposium for Testing and Failure Analysis, Nov. 15-19, 1998, 5 pages.
- Bodoh, Dan, "Publish Failure-Analysis Reports on the Web," Test & Measurement World, Sep. 1, 1999, 7 pages.
- Borman, D., "Telnet Authentication: Kerberos Version 4," Request for Comments 1411, Jan. 1993, pp. 1-4.
- Chaum, David, "Achieving Electronic Privacy," Scientific American, Aug. 1992, pp. 96-101.
- Fiat, Amos, et al. "How to Prove Yourself: Practical Solutions to Identification and Signature Problems," Lecture Notes in Computer Science, Aug. 11, 1986, pp. 186-194.
- GIF Wizard, "Accelerate your website!," <http://uswest.gifwizard.com>, Jan. 11, 1998 accessed via the wayback machine.
- GIF Wizard, "GIF Wizard Single URL/File Compression," <http://uswest.gifwizard.com/PGW?task=singleurlfile&SP=wmgFdUAZE26dbTeZes>, Jan. 11, 1998 accessed via the wayback machine.
- Griswold, Gary N., "A Method for Protecting Copyright on Networks," Interactive Multimedia Association Intellectual Property Proceedings, Apr. 2-3, 1993.
- Grover, Derrick, eds., "The Protection of Computer Software—its Technology and Applications," 1989, 1990, 1992.
- Herzberg, Amir, et al., "Public Protection of Software," ACM Transactions on Computer Systems, vol. 5, No. 4, Nov. 1987, pp. 371-393.
- "id Software's QUAKE to Explode Online and at Retail; For the First Time, id Will Distribute Their Own Game at Retail; Shareware Version to Contain Full Version Encrypted on CD-ROM," Business Wire, May 13, 1996, 2 pages.
- Lampson, Butler W., "Authentication and Delegation with Smart-Cards," Oct. 22, 1990.
- Lampson, "Computers at Risk," 1991, 2 cover pages and pp. 74-101.
- Lampson, Butler W., "Requirements and Technology for Computer Security," Jul. 1990, 65 pages.
- McMahon, P.V., "SESAME V2 Public Key and Authorisation Extensions to Kerberos," IEEE, 1995, pp. 114-131.
- Miller, S.P., et al., "Kerberos Authentication and Authorization System," Project Athena Technical Plan, Oct. 27, 1988, pp. 1-36.
- Neuman, B. Clifford, et al., "Kerberos: An Authentication Service for Computer Networks," IEEE Communications Magazine, vol. 32, No. 9, Sep. 1994, 11 pages.
- "Overpowered by Generosity," New Scientist, Aug. 13, 1994, pp. 43 and 44.
- Phipps, John, "Physical Protection Devices," The Protection of Computer Software—it's Technology and Applications, Second edition, 1992, 2 cover pages and pp. 61-81.
- Purdy, George B., et al., "A Software Protection Scheme," Proceedings for the 1982 Symposium on Security and Privacy Apr. 26-28, 1982, 2 cover pages and pp. 99-103.
- Rigney, C., et al., "Remote Authentication Dial in User Service (RADIUS)," Network Working Group Request for Comments 2865, Jun. 2000, pp. 1-76.
- Shamir, Adi, "Identity-based Cryptosystems and Signature Schemes," Lecture Notes in Computer Science, 1985, 2 cover pages and pp. 47-53.
- SPA, "Electronics Software Distribution Policies for Software Publishers," Oct. 7, 1996, 26 pages.
- Steiner, Jennifer, et al., "Kerberos: An Authentication Service for Open Network Systems," Jan. 12, 1988, pp. 1-15.
- "Transmitting large color files," The Seybold Report on Publishing Systems, Oct. 26, 1994, 9 pages.
- Webb, Joseph A., "CD-ROM Expo: Developing with the Industry," Information Today, vol. 6, Issue 10, Nov. 1989, pp. 1, 3, 29, and 30.
- White, Steve R., et al., "ABYSS: A Trusted Architecture for Software Protection," Proceedings 1987 IEEE Symposium on Security and Privacy, Apr. 27-29, 1987, 2 cover pages and pp. 38-51.
- Willens, S., et al., "Remote Authentication Dial in User Service (RADIUS) draft-ietf-nasreq-radius-01.txt (c)," Network Working Group Internet Draft, May 1994, 74 pages.
- Rainbow Technologies; iKey 1000 Series Product Brief; Rev. 1.1; Apr. 27, 2001; 7 pages.
- Rigney, C.; RFC 2139—RADIUS Accounting; Apr. 1997; 25 pages.
- U.S. Department of Commerce/National Institute of Standards and Technology; FIPS PUB 190—Guideline for the Use of Advanced Authentication Technology Alternatives; Sep. 1994; 47 pages.
- Prism Technologies, LLC's Objections and Responses to Defendants' First Set of Common Requests for Admission (Nos. 1-18); *Prism Technologies, LLC v. Adobe Systems Inc., et al.*; Case No. 8:10-cv-00220-LES-TDT; dated Mar. 26, 2012; 10 pages.
- Andrews, Whit; "Financial Trader Looks Past IBM to Startup for Secure Transactions," Marketing & Commerce; Jul. 7, 1997; 1 page.
- Ascend Communications; "MAX T1/PRI RADIUS Supplement;" Jan. 24, 1996; 85 pages.
- Ascend Communications; "MAX T1/PRI Security Supplement;" Jan. 25, 1996; 44 pages.
- Business Wire; "Security Dynamics to Enhance Network Security for Oracle Universal Server; Security Dynamics is First Provider of Token-Based User Authentication Technology for Oracle7's Advanced Networking Option," Feb. 26, 1996; 2 pages.
- European Telecommunications Standards Institute; "European Digital Cellular Telecommunications System (Phase 1); Security-Related Network Functions (GSM 03.20);" Feb. 1992; 45 pages.
- European Telecommunications Standards Institute; "European Digital Cellular Telecommunications System (Phase 2); Mobile Application Part (MAP) Specification (GSM 09.02);" 1995; 804 pages.
- European Telecommunications Standards Institute; "European Digital Cellular Telecommunications System (Phase 2); Mobile-Services Switching Centre-Base Station System (MSC-BBS) Interface Layer 3 Specification (GSM 08.08);" 1995; 104 pages.
- Gregg, Rick; "email to Sandeep Giri and Tim Goeke, Re: Site Testing;" Jun. 15, 1996; 3 pages.
- Krajewski Jr., Marjan; "Concept for a Smart Card Kerberos," Oct. 16, 1992; pp. 76-83.
- "Oracle Advanced Networking Option Administrator's Guide;" Copyright 1996; 140 pages.

**US 8,387,155 B2**

Page 19

---

"Oracle7 Server Concepts Manual;" Copyright 1996; 88 pages.  
RADIUS IETF Mailing List; downloaded from <http://ftp.cerias.purdue.edu/pub/doc/network/radius/archive/ietf-radius.9511>; dated Nov. 1, 1995; 162 pages.  
Prism Resources; "Internet Copyright Protection;" Jan. 3, 1997; 2 pages.  
Scourias, John; "Overview of the Global System for Mobile Communications;" Oct. 14, 1997; 15 pages.

"Security Dynamics Introduces SecurID Modem;" Sep. 19, 2000; 2 pages.  
Shostack, Adam; "Apparent Weaknesses in the Security Dynamics Client/Server Protocol;" Oct. 1996; 6 pages.  
"Understanding SQL\*Net;" copyright 1996; 82 pages.

\* cited by examiner

**TX0002-0021**

Appx195

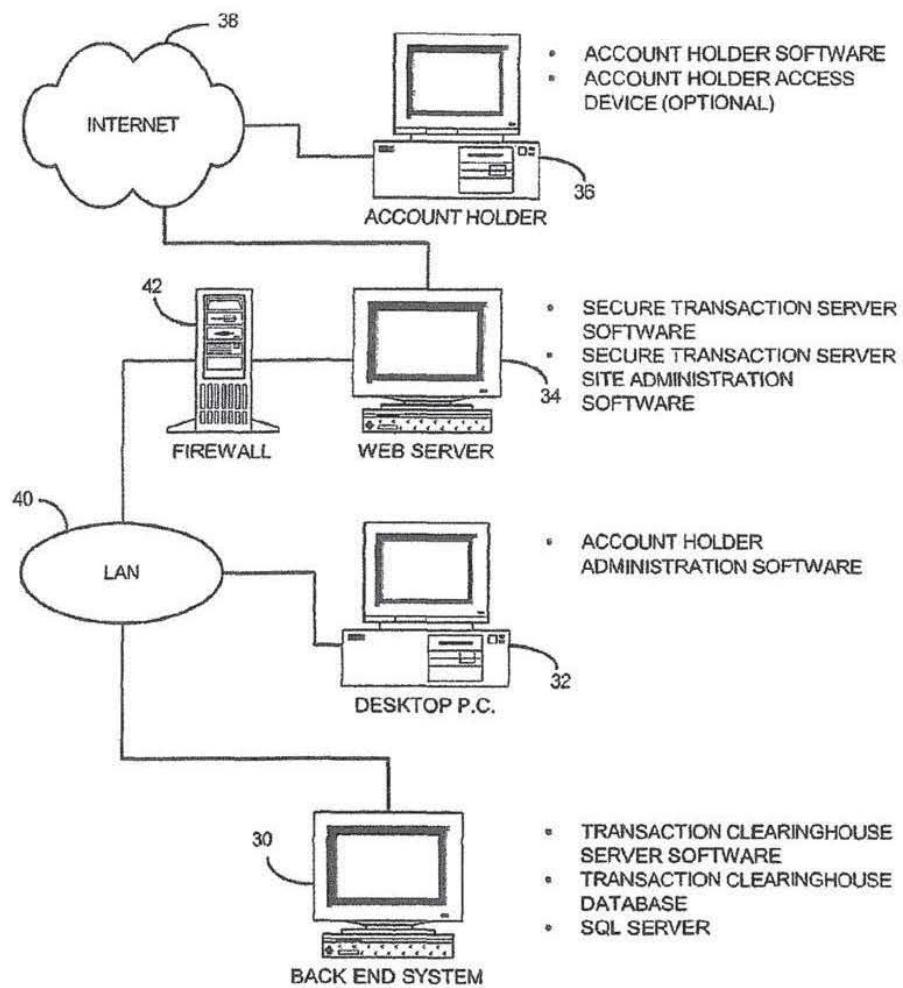


FIG. 1

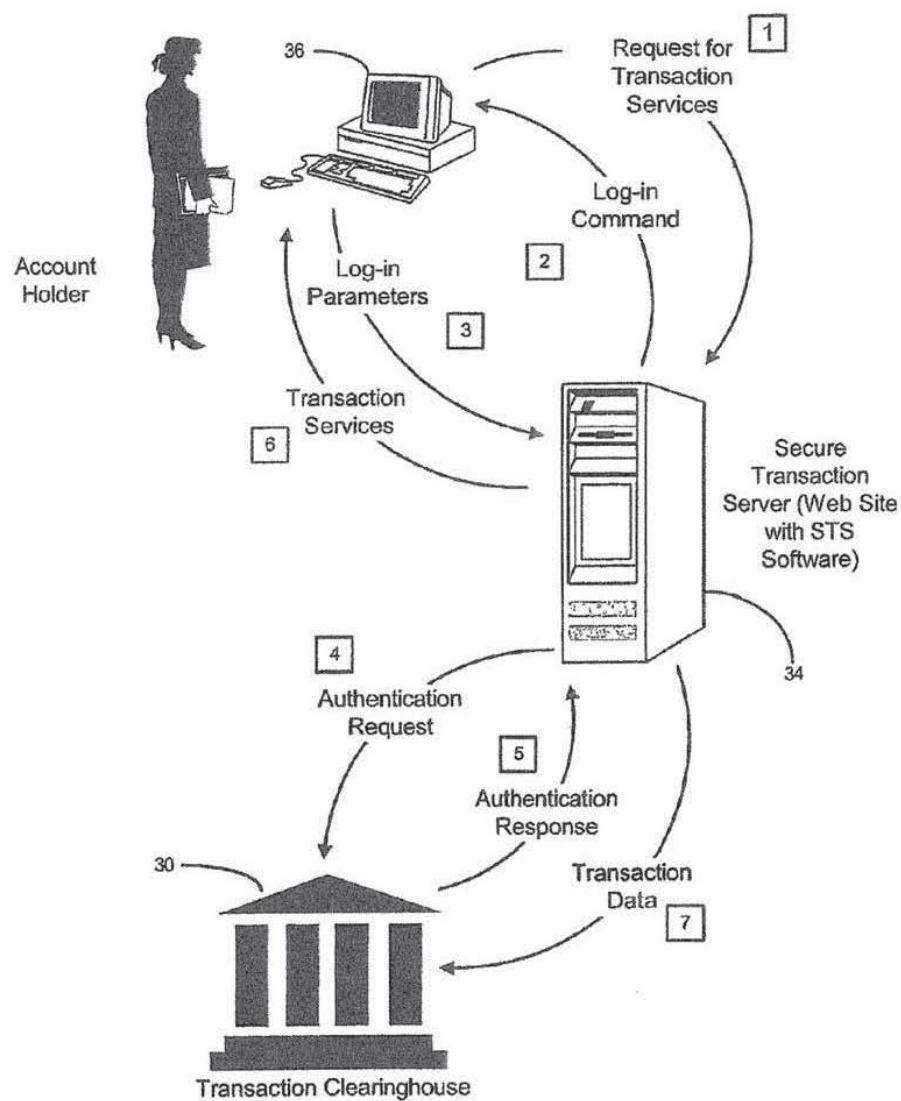


FIG. 2

TX0002-0023

Appx197

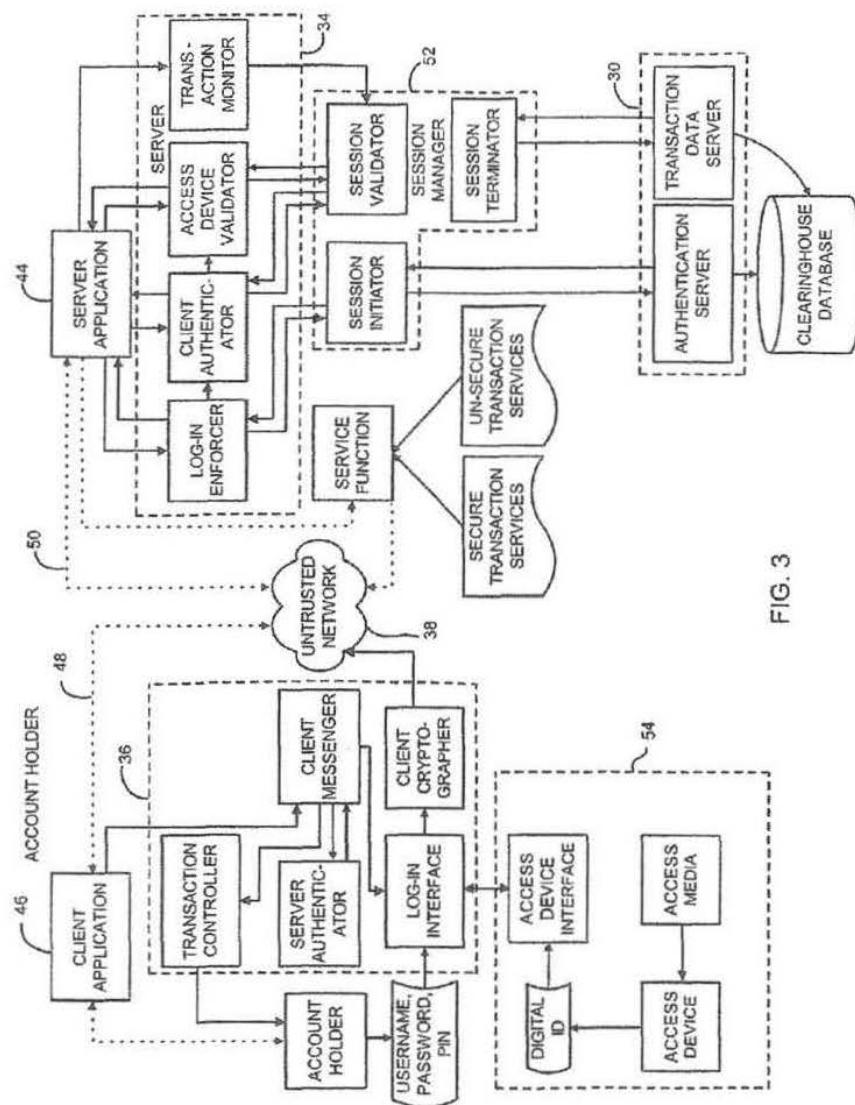
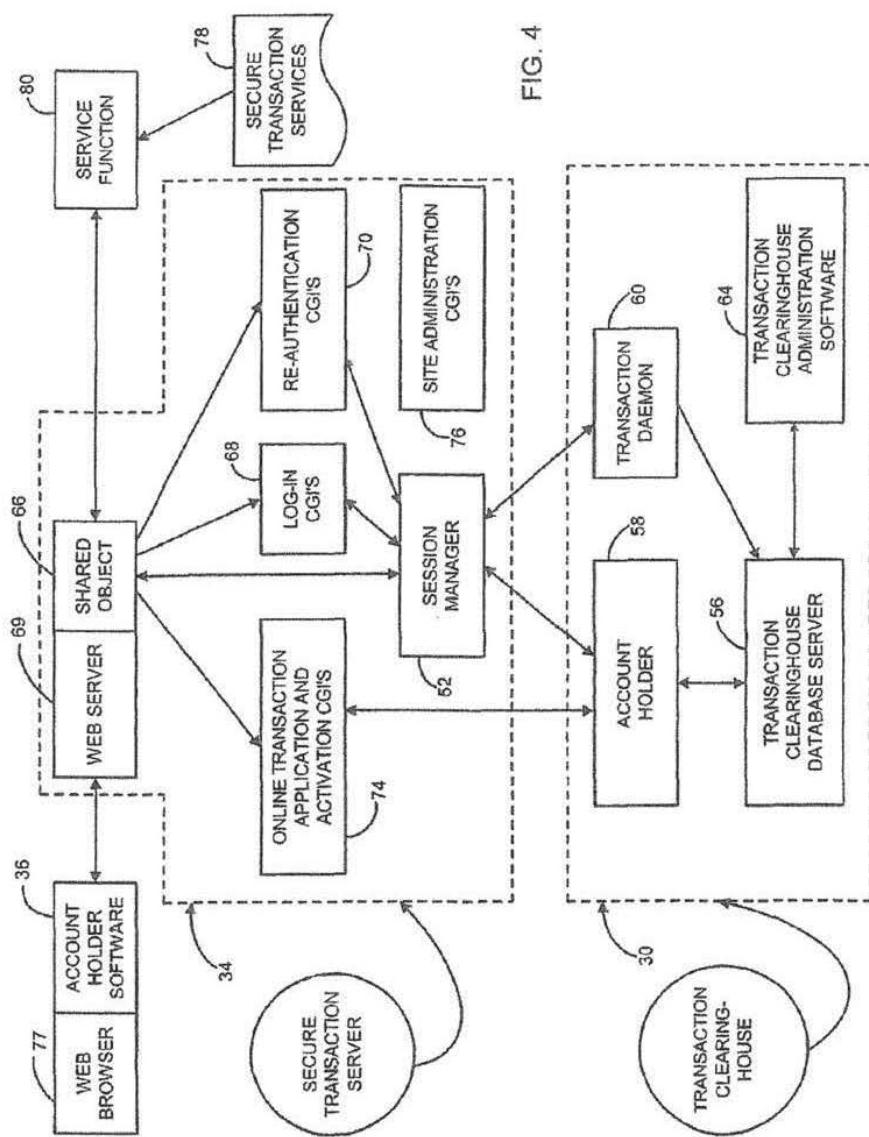


FIG. 3



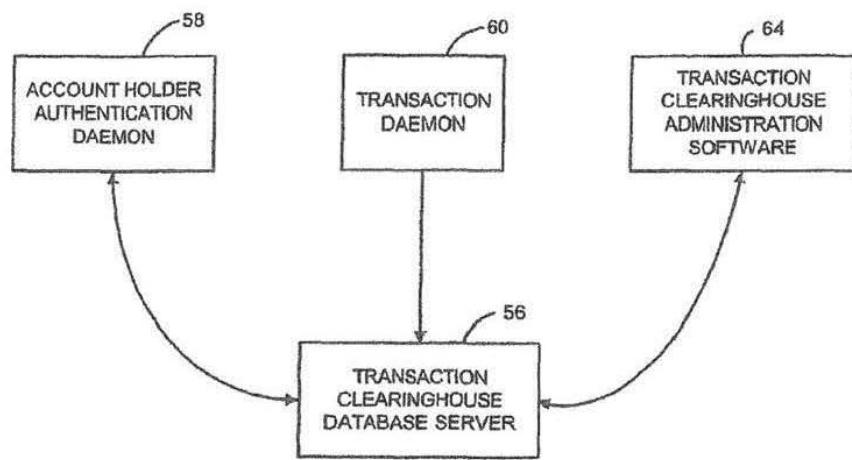


FIG. 5

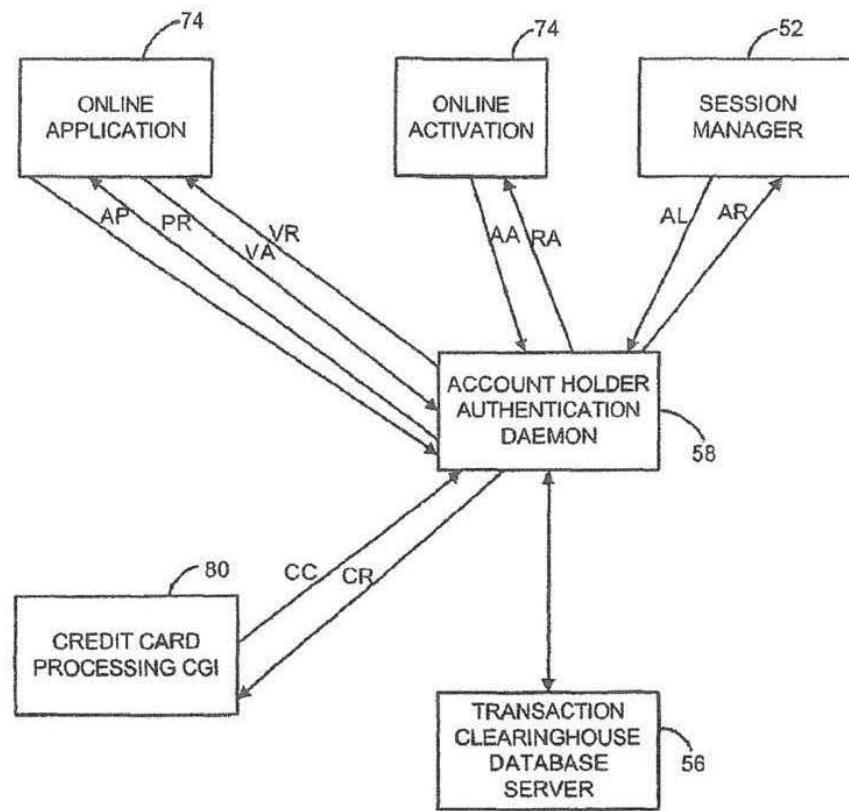


FIG. 6

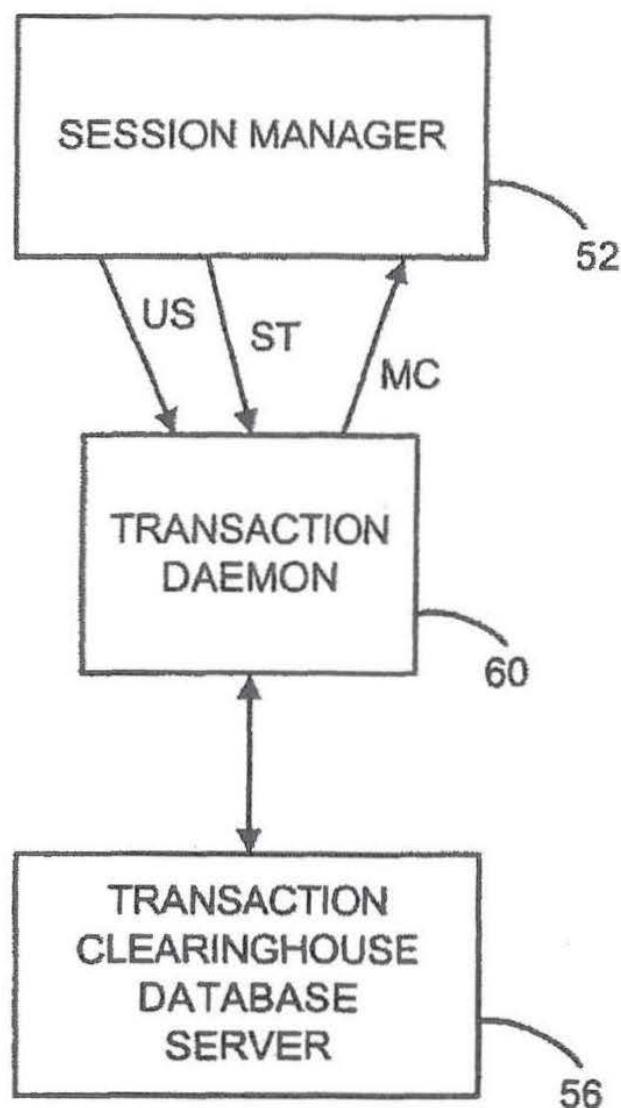


FIG. 7

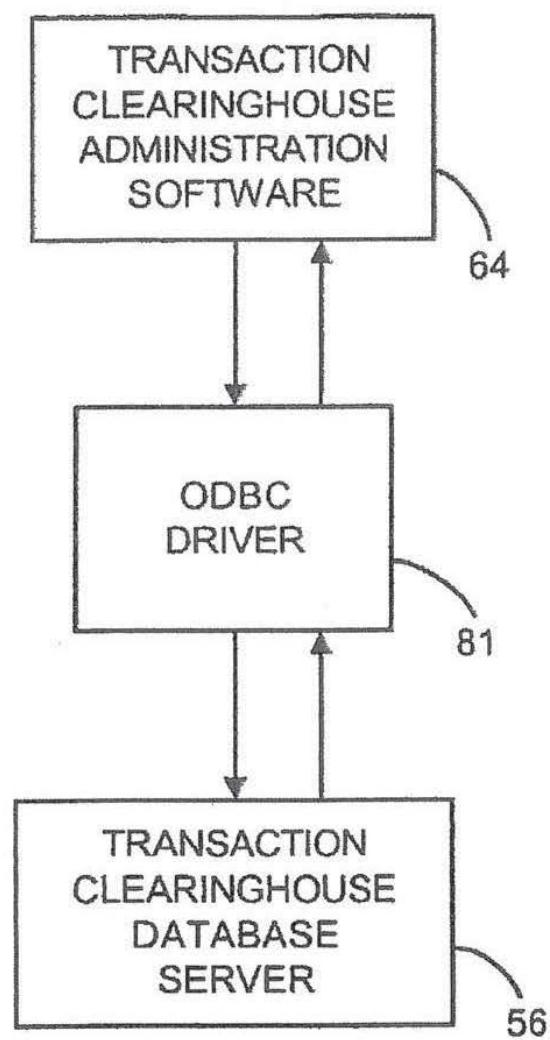


FIG. 8

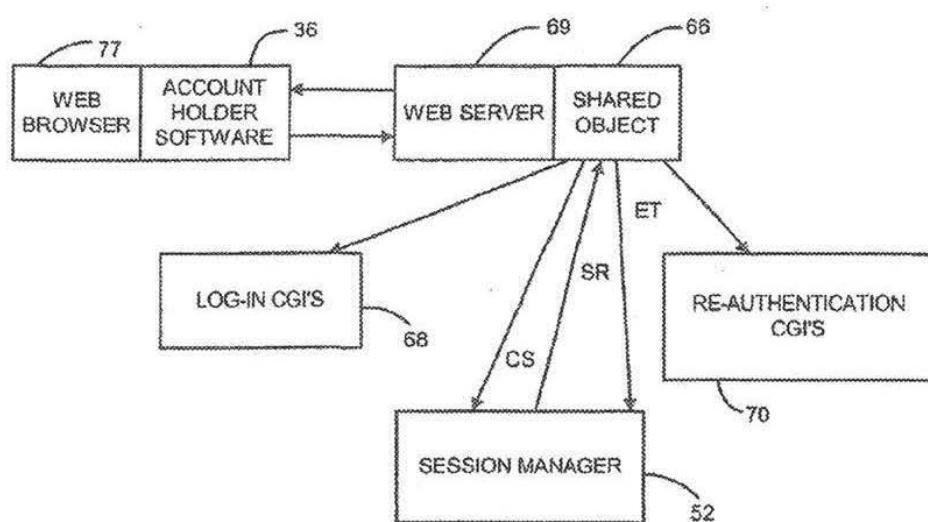


FIG. 9

TX0002-0030

Appx204

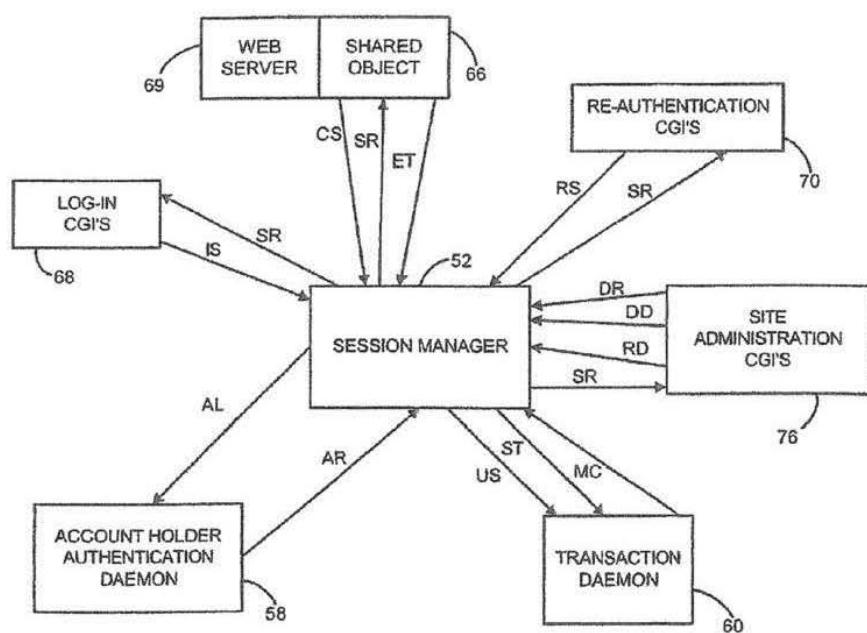


FIG. 10

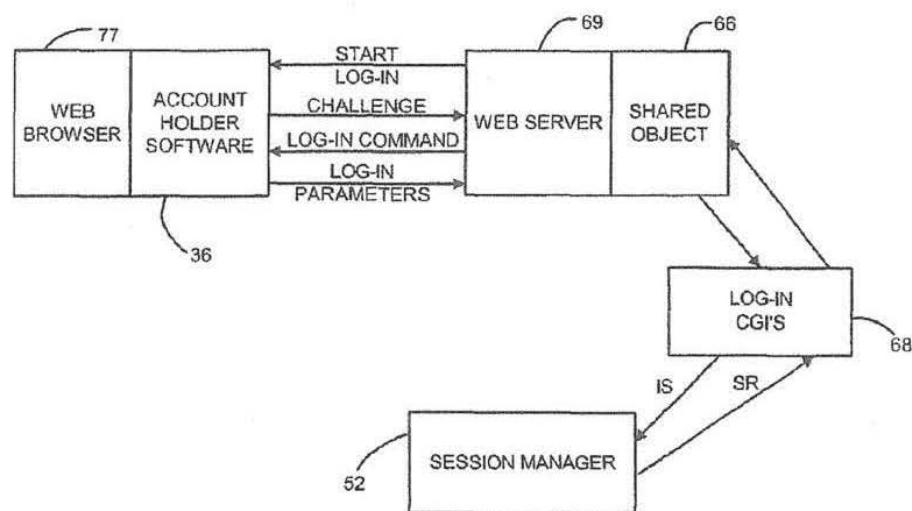


FIG. 11

TX0002-0032

Appx206

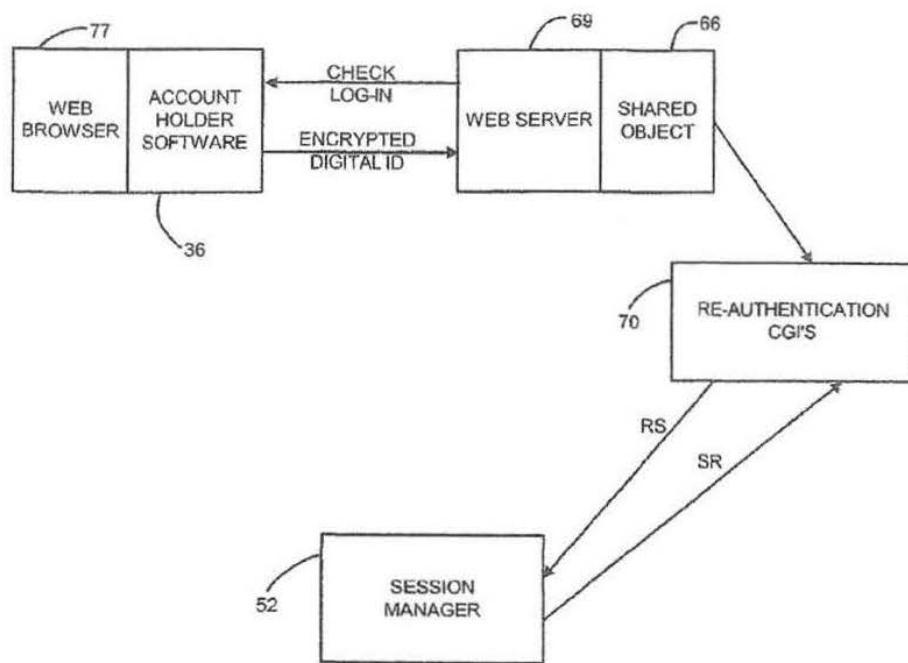


FIG. 12

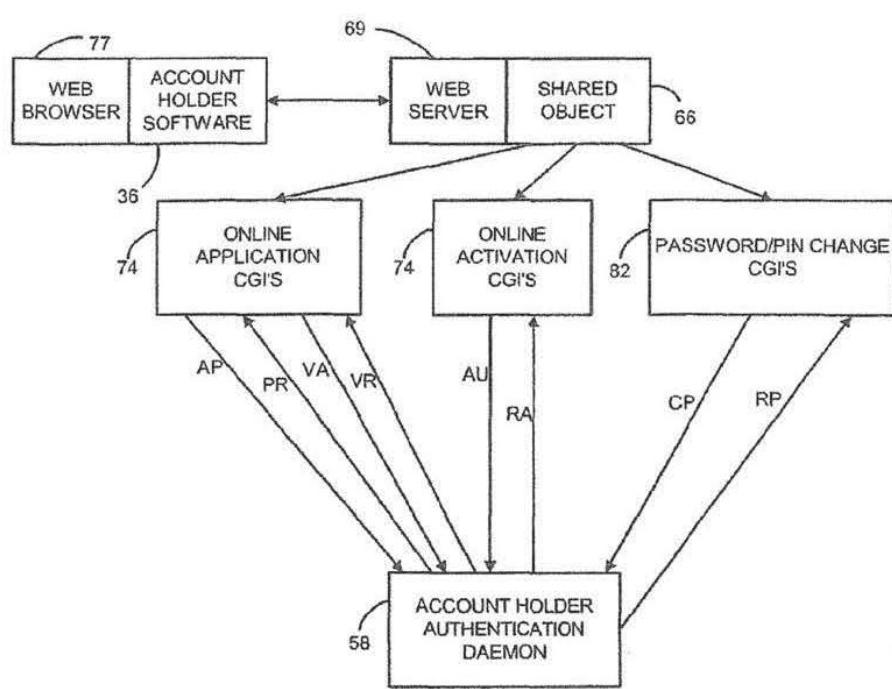


FIG. 13

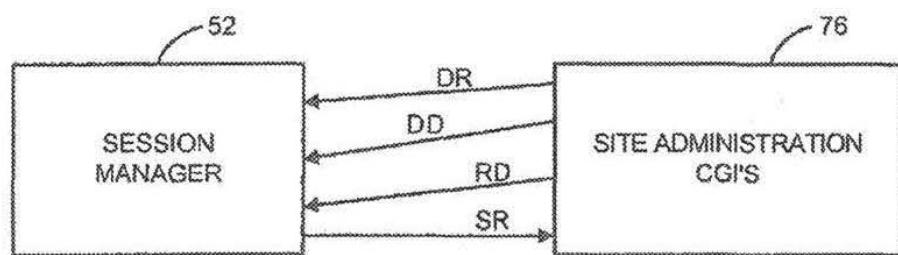
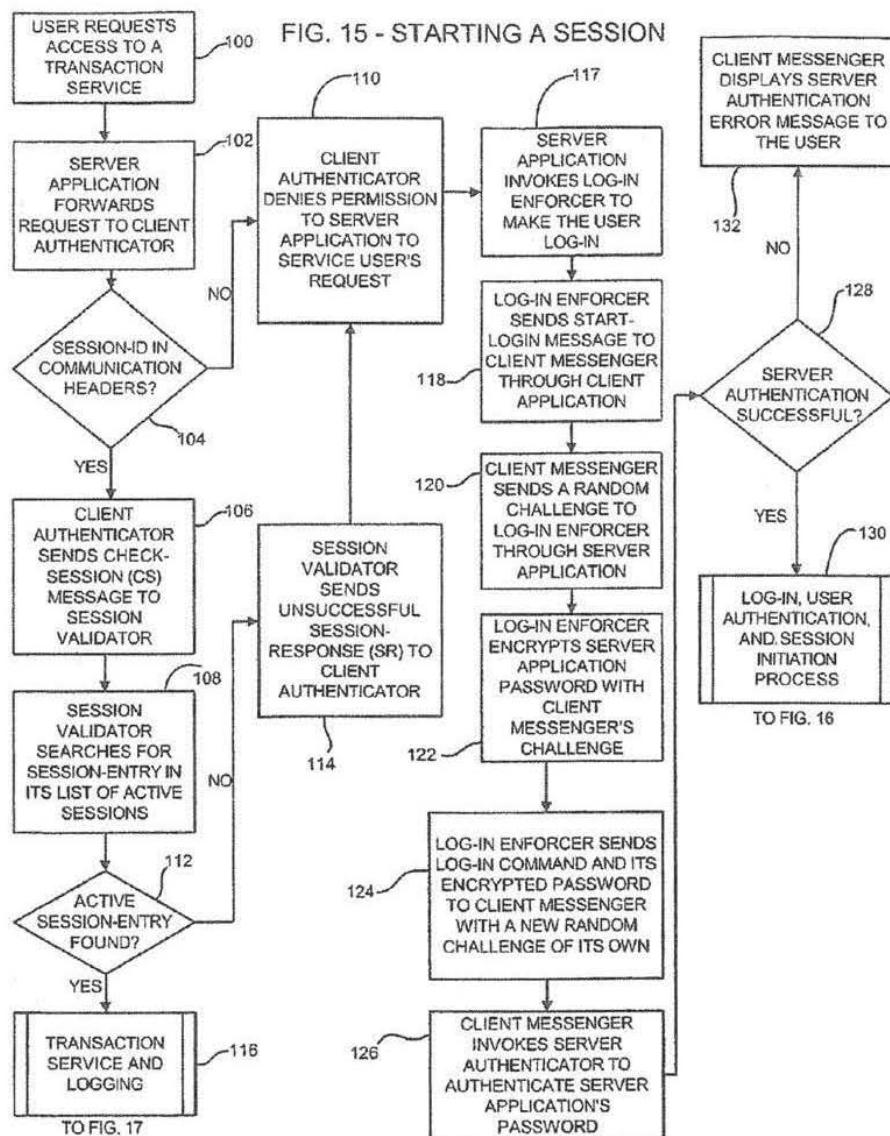
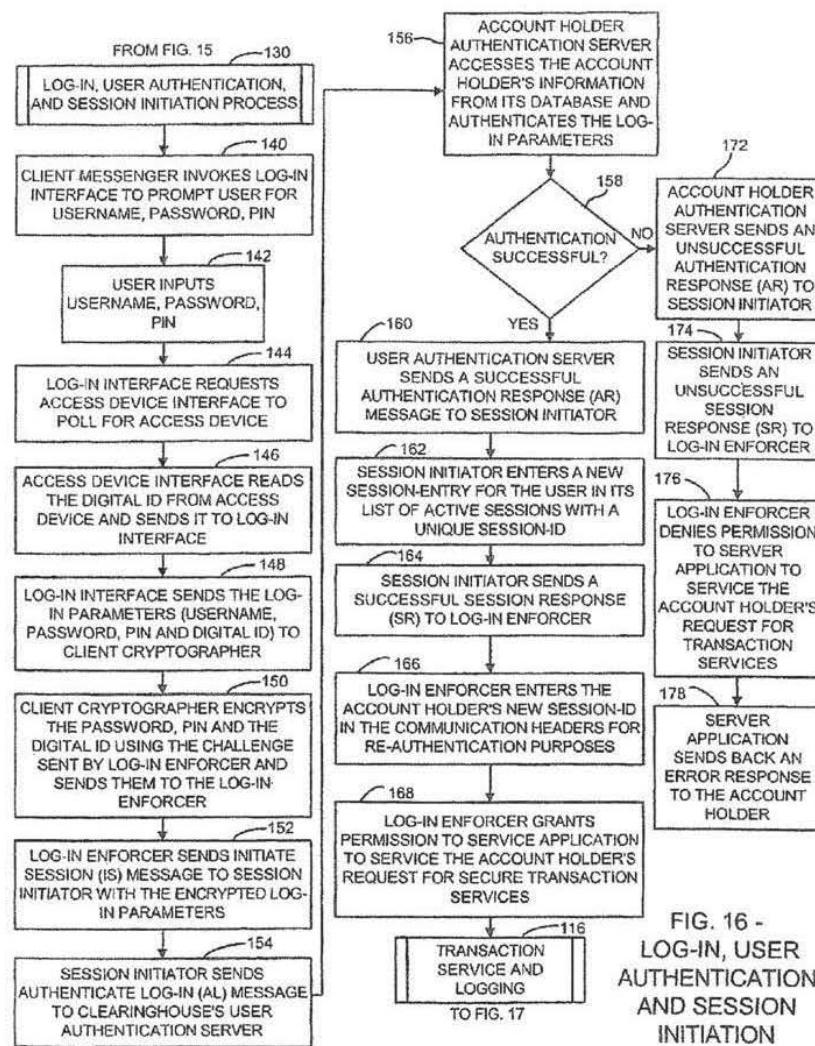


FIG. 14





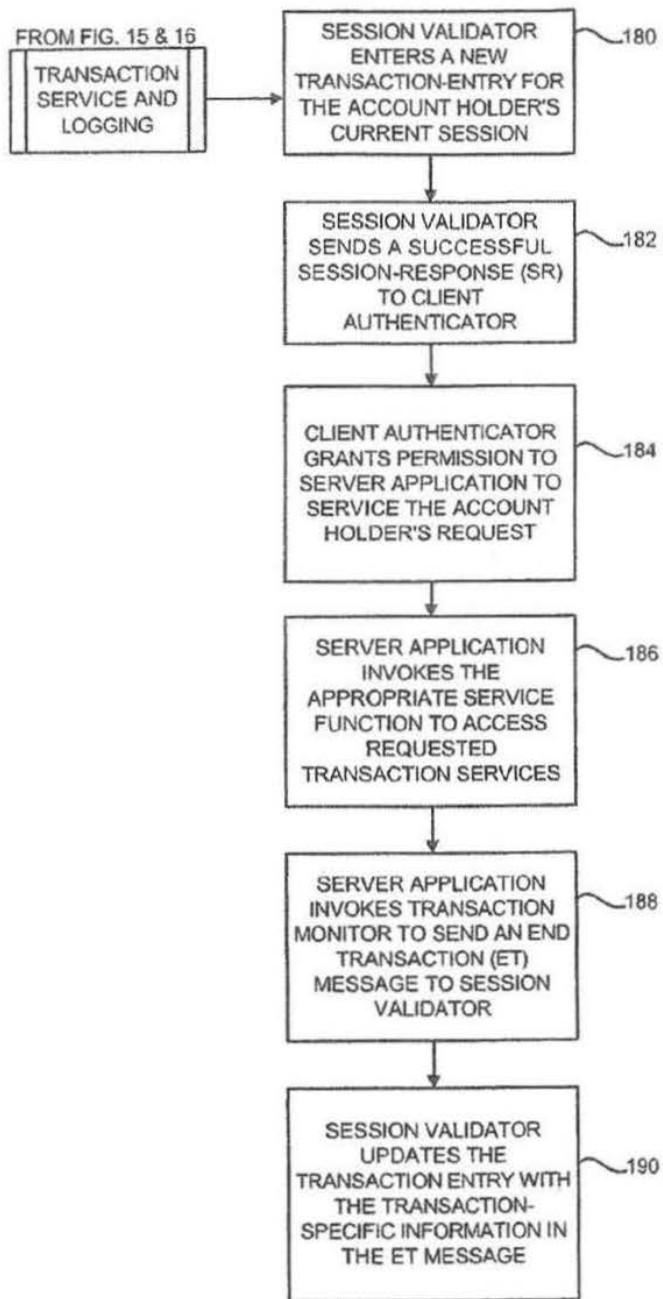
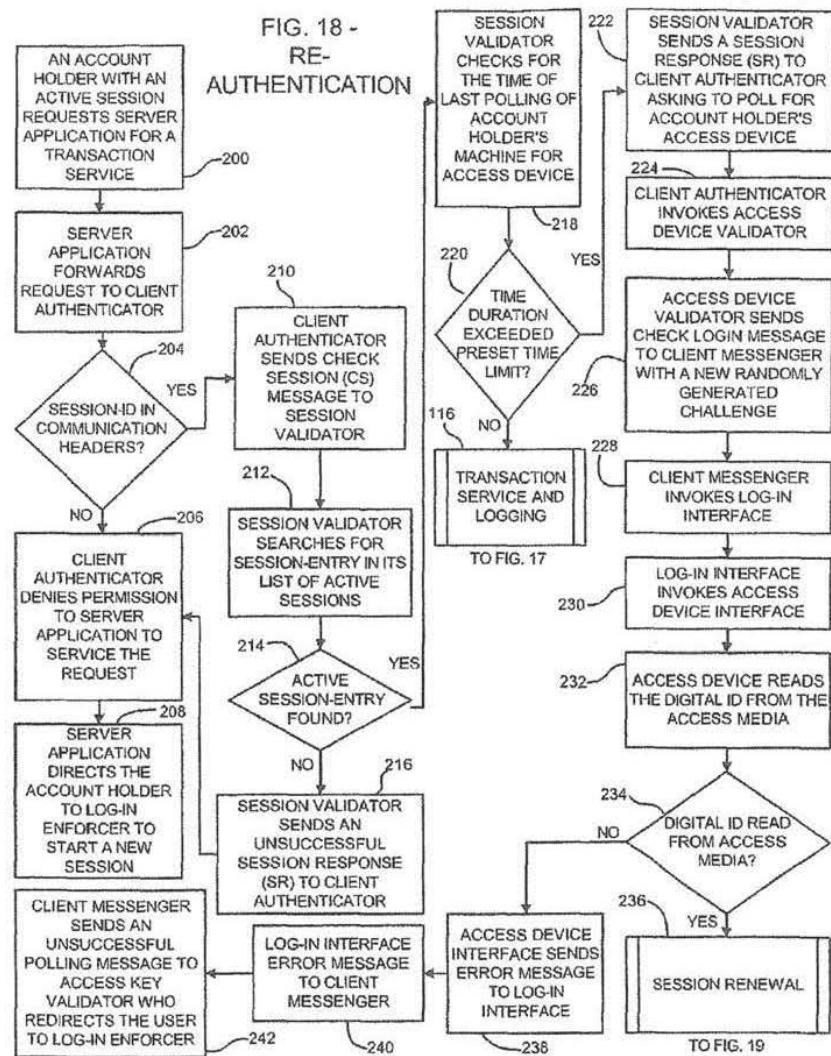
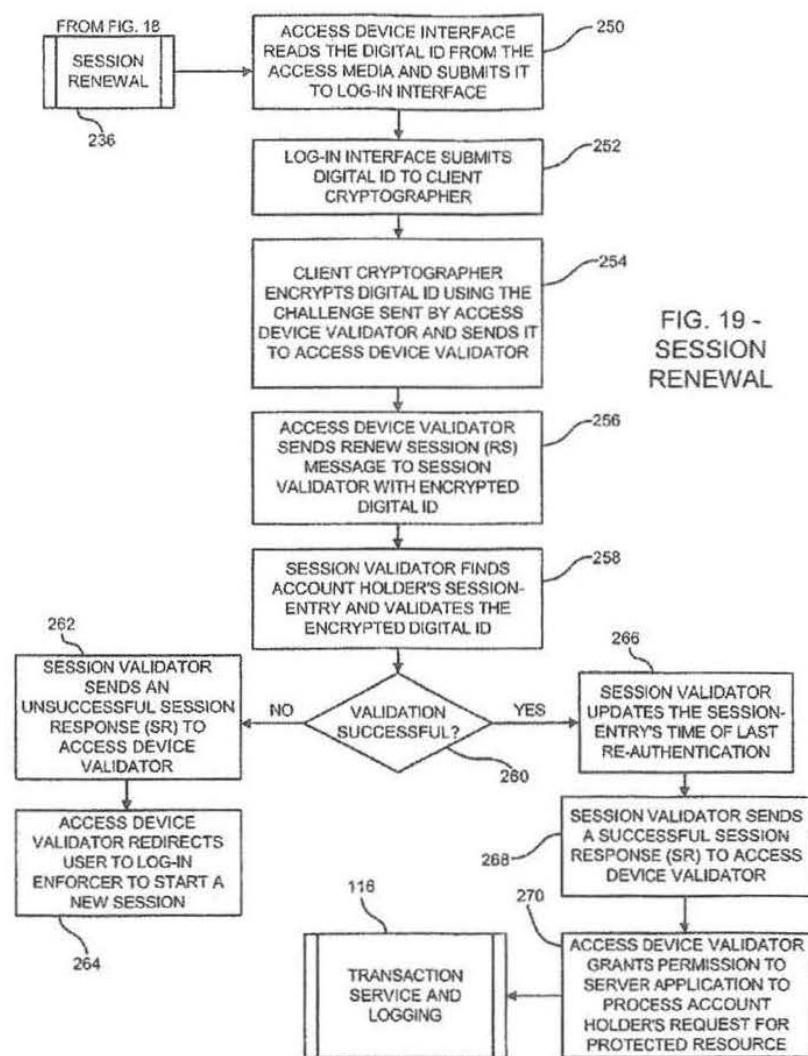
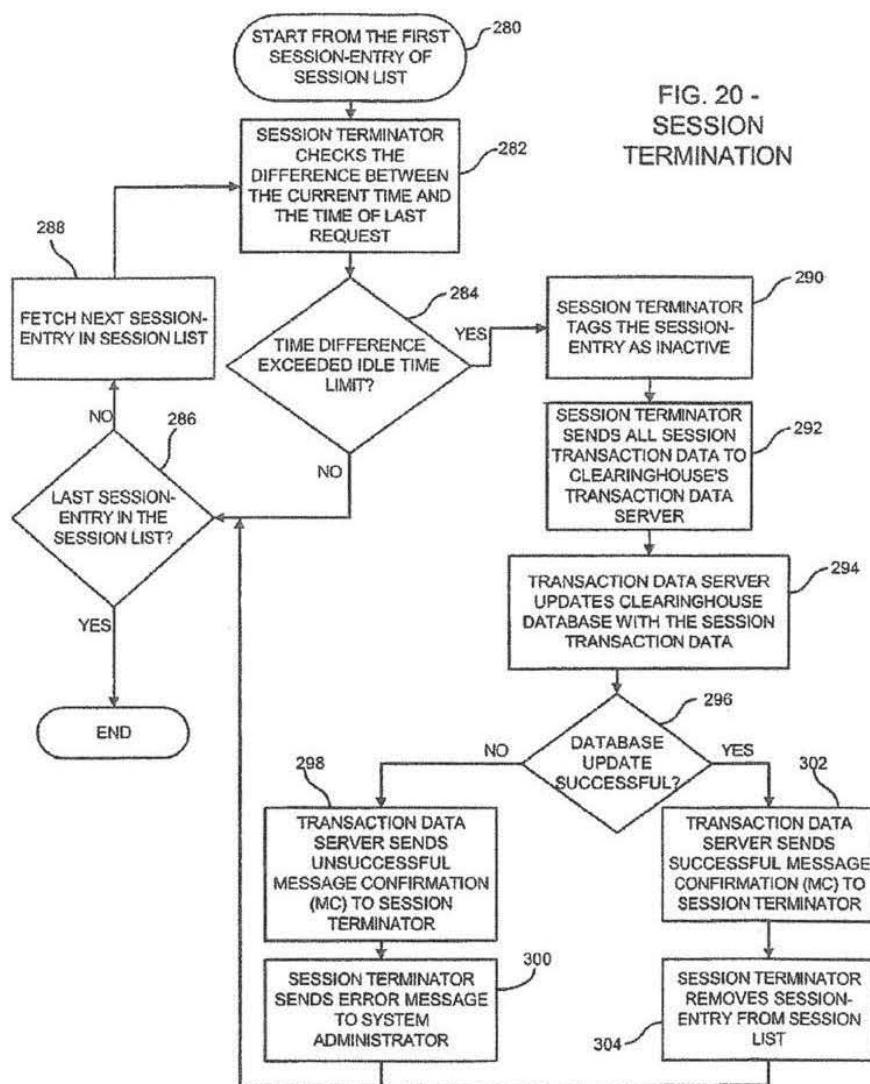


FIG. 17 - TRANSACTION SERVICE AND LOGGING

TX0002-0038







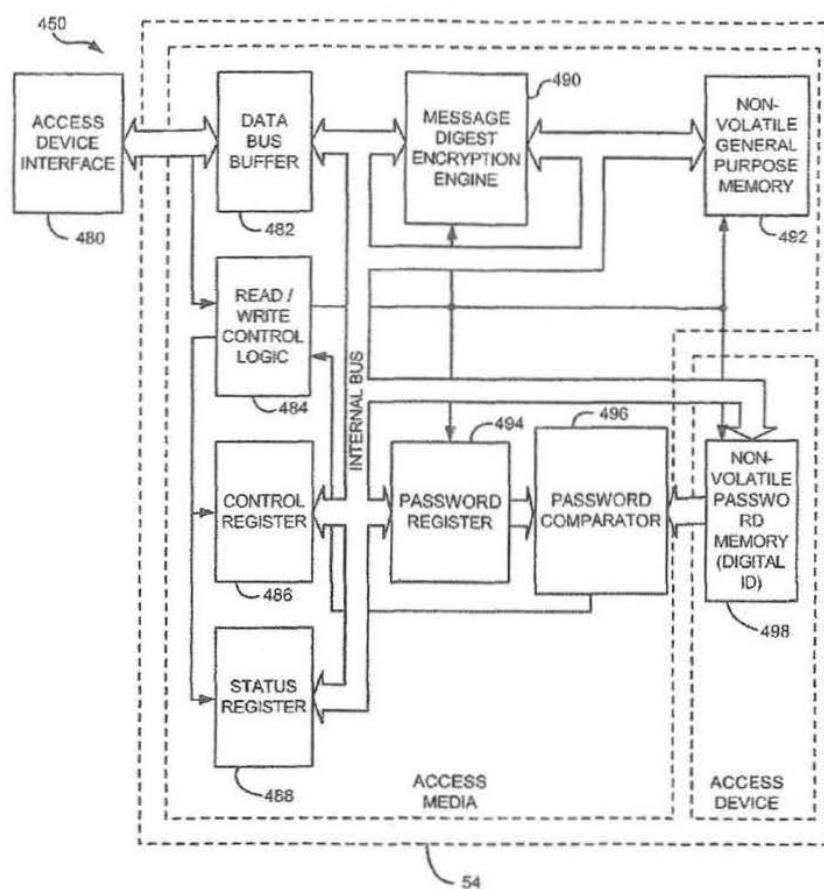


FIG. 21 -  
HARDWARE TOKEN  
ACCESS DEVICE

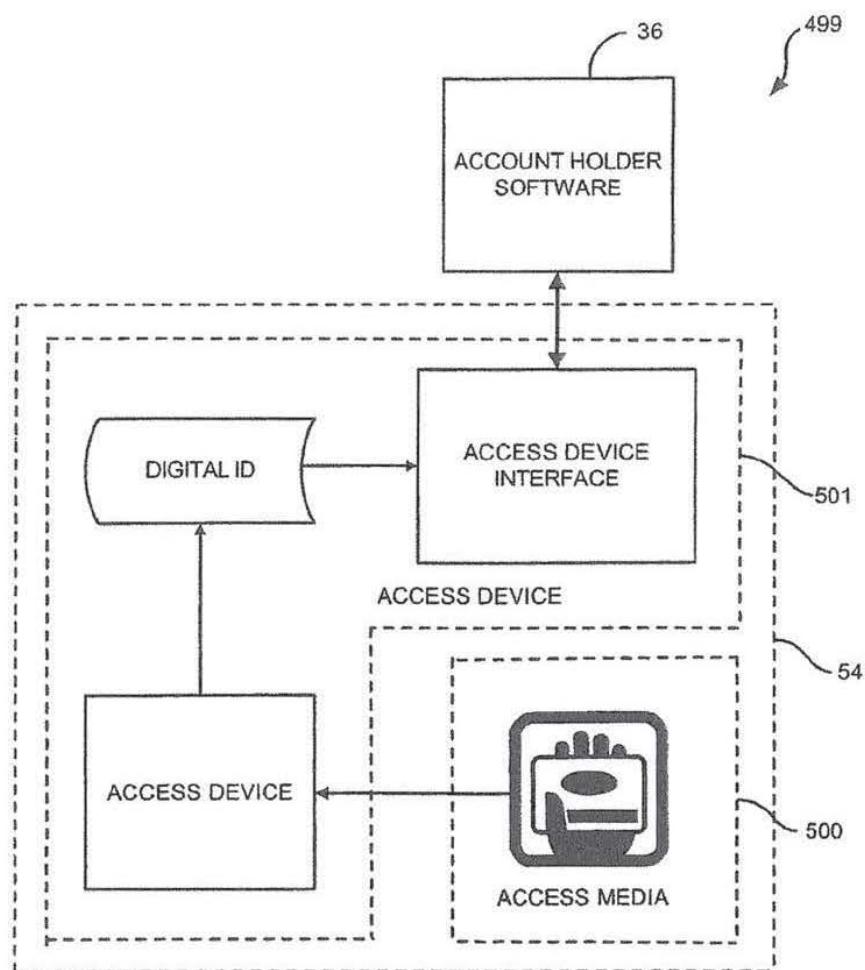


FIG. 22 -  
MAGNETIC CARD ACCESS DEVICE

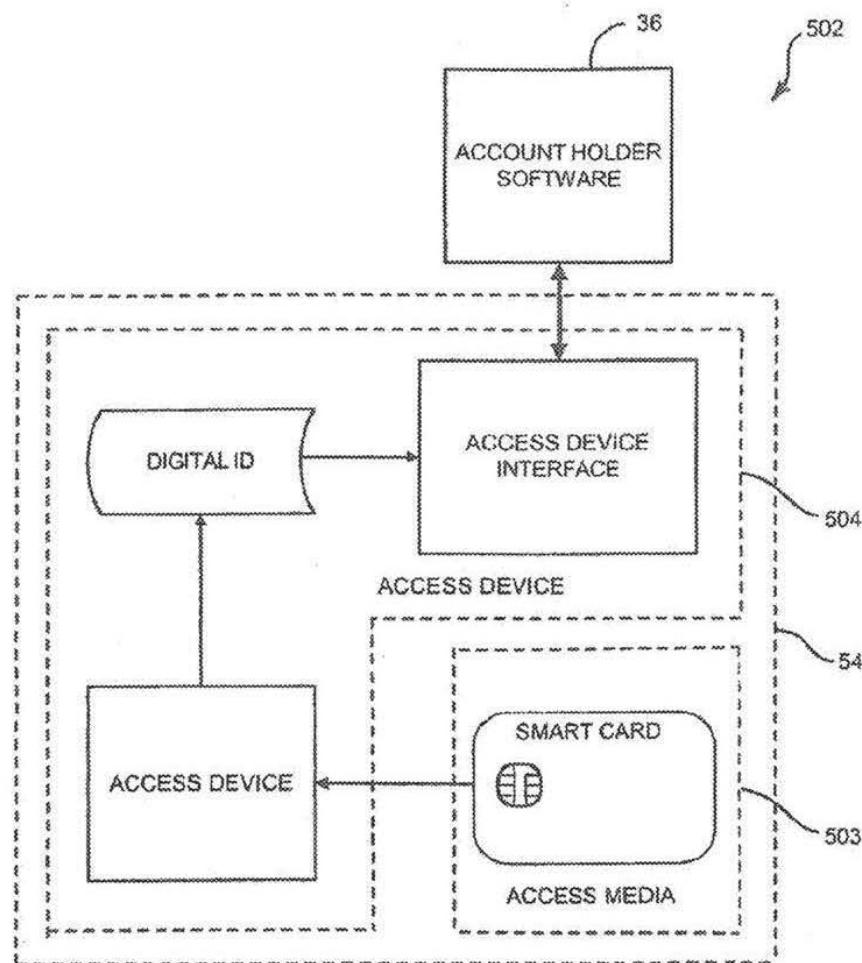


FIG. 23 -  
SMART CARD ACCESS DEVICE

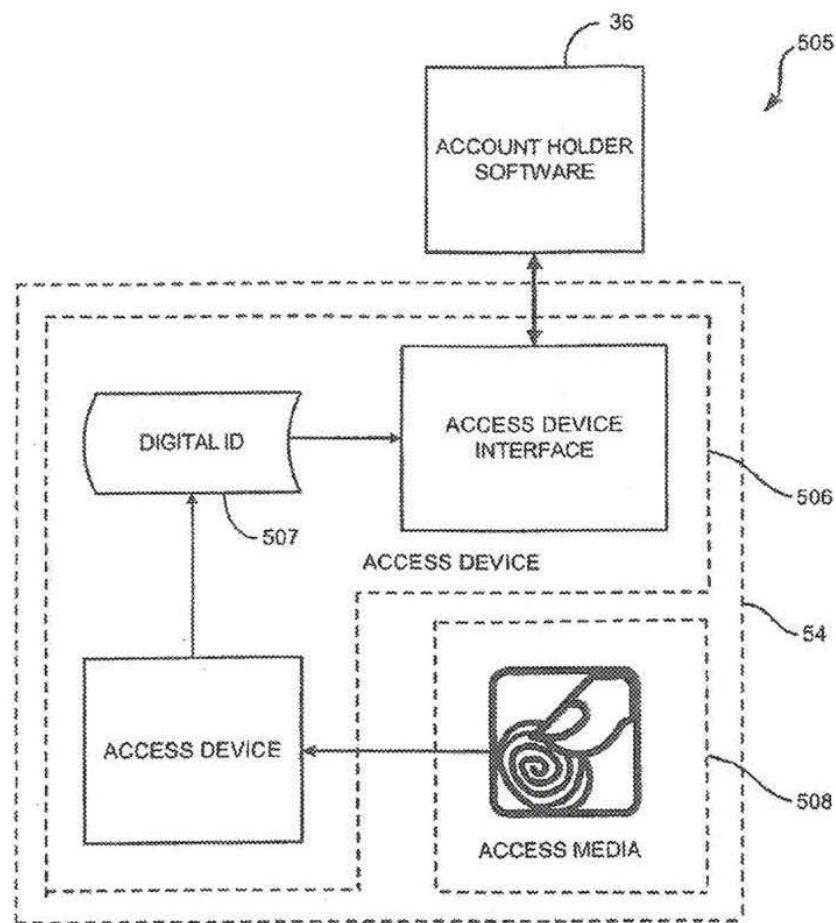


FIG. 24 -  
BIOMETRIC IDENTIFICATION ACCESS DEVICE

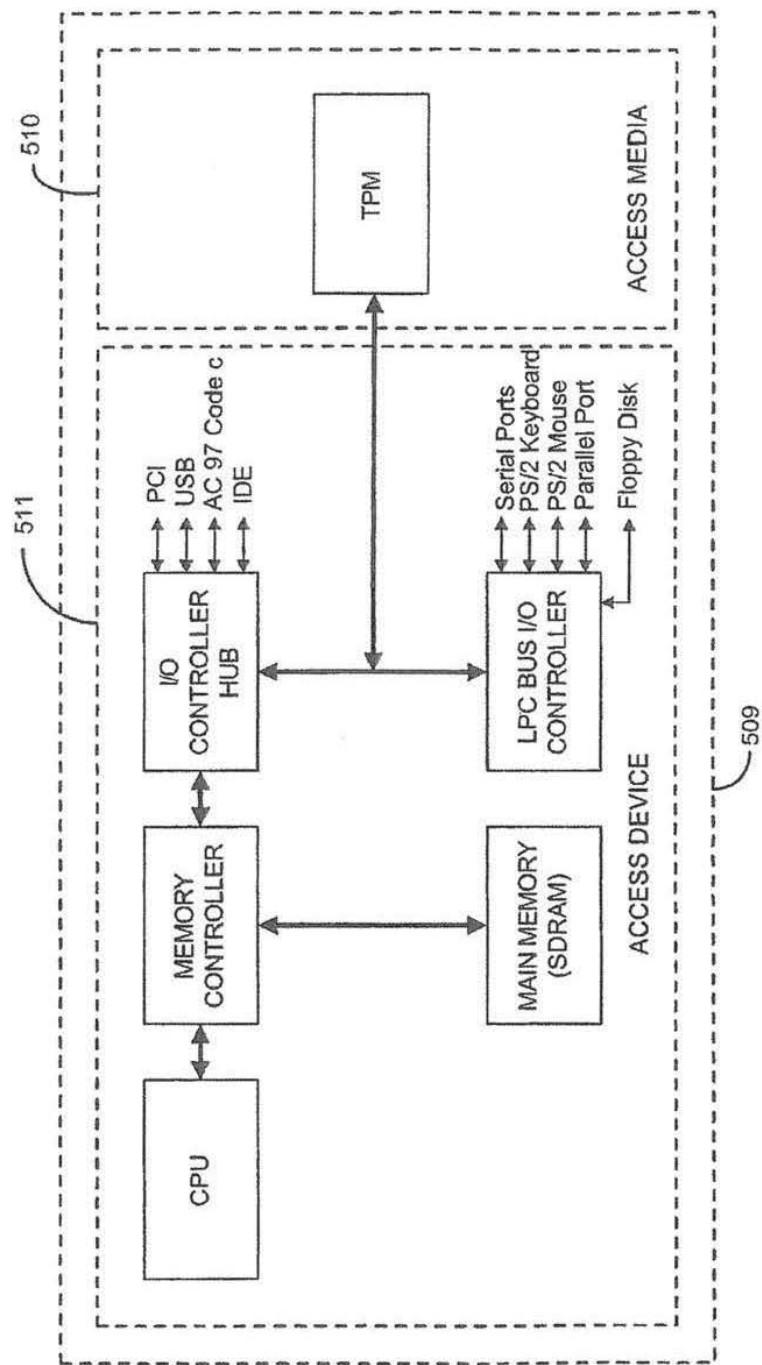


FIG. 25 -  
SECURE CENTRAL PROCESSING UNIT (CPU) ACCESS DRIVE

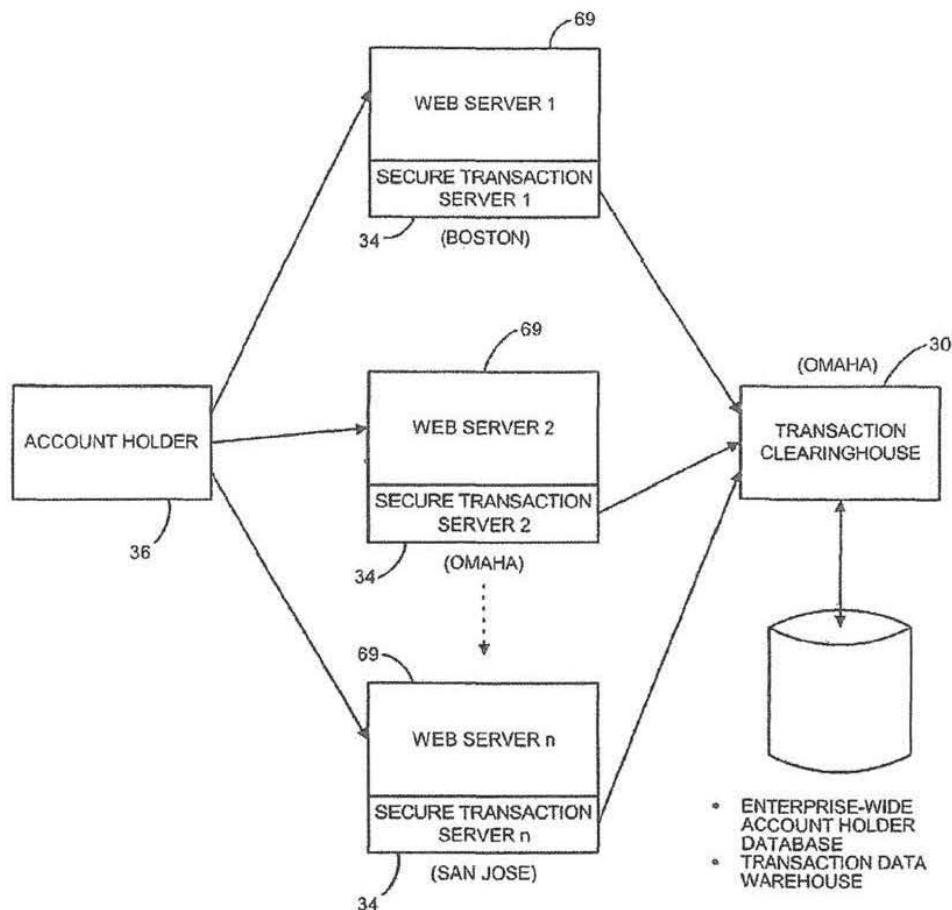


FIG. 26 -  
MULTIPLE SECURE TRANSACTION SERVERS WITH A  
SINGLE TRANSACTION CLEARINGHOUSE

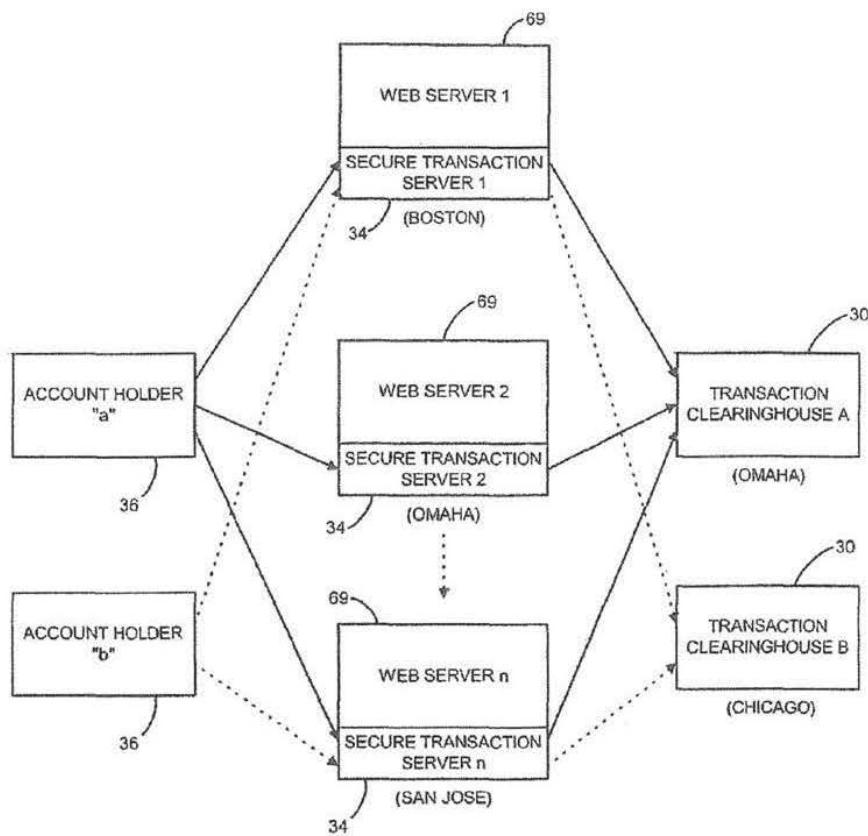


FIG. 27 -  
MULTIPLE SECURE TRANSACTION SERVERS WITH  
MULTIPLE TRANSACTION CLEARINGHOUSES

**1****SYSTEM FOR MANAGING ACCESS TO PROTECTED COMPUTER RESOURCES**

The present application is a continuation of application Ser. No. 11/978,919, filed Oct. 30, 2007 now U.S. Pat. No. 8,127,345; which is a continuation of application Ser. No. 10/230,638, filed Aug. 29, 2002, now U.S. Pat. No. 7,290,288; which are incorporated herein by reference; and which is a continuation-in-part of application Ser. No. 08/872,710, filed Jun. 11, 1997, now U.S. Pat. No. 6,516,416.

**BACKGROUND OF THE INVENTION****1. Field of the Invention**

The present invention generally relates to security systems for use with computer networks. More particularly, the present invention relates to a secure transaction system that is particularly adapted for use with untrusted networks, such as the Internet.

**2. Description of the Prior Art**

There are many businesses that are connected to the Internet or some other untrusted network. Such businesses may provide transaction services without charge for certain transactions that can be accessed by any account holder having access to the network. However, the same business may want to generate revenue from other transaction services and also to protect its business assets. In order to generate revenue, there must be control over account holder access, transaction tracking, account data, and billing. For a business to offer transaction services on an untrusted network, such as the web, it must have access to a web server that connects to the Internet. Any account holder with a web browser can then access the web site.

To implement a secure transaction system for use over the web, businesses need to implement authentication, authorization and transaction tracking. Authentication involves providing restricted access to transaction services that are made available, and this is typically implemented through traditional account holder name-password schemes. Such schemes are vulnerable to password fraud because account holders can share their usernames and password by word of mouth or through Internet news groups, which obviously is conducive to fraudulent access and loss of revenue. Authorization, on the other hand, enables authenticated account holders to access transaction services based on the permission level they are granted. Transaction tracking involves collecting information on how account holders are using a particular web site, which traditionally involved the data mining of web server logs. This information is often inadequate to link web site transaction and a particular account holder who used the web site. There is also no generic transaction model that defines a web transaction, which contributes to the difficulty in implementing an account holder model based upon transactions. Thus, there is a need for an improved secure transaction system and method for securing and tracking usage by a client computer.

**SUMMARY OF THE INVENTION**

The present invention discloses a system for securing and tracking usage of transaction services or computer resources by a client computer from a first server computer, which includes clearinghouse means for storing identity data of the first server computer and the client computer(s); server software means installed on the first server computer and client software means installed on the client computer(s) adapted to forward its identity data and identity data of the client com-

**2**

puter(s) to the clearinghouse means at the beginning of an operating session; and a hardware key connected to the client computer, the key being adapted to generate a digital identification as part of the identity data; the server software means being adapted to selectively request the client computer to forward the identification to the first server computer for confirmation of the hardware key being connected; the clearinghouse means being adapted to authenticate the identity of the client computer responsive to a request for selected services or resources of the first server computer; the clearinghouse means being adapted to authenticate the identity of the first server computer responsive to the client computer making the request; and the clearinghouse means being adapted to permit access to the selected request responsive to successful initial authentication of the first server computer and the client computer making the request; wherein the hardware key is implemented using a hardware token access system, a magnetic card access system, a smart card access system, a biometric identification access system or a central processing unit with a unique embedded digital identification.

These and other objects of the present invention will be apparent from review of the following specification and the accompanying drawings.

**BRIEF DESCRIPTION OF THE DRAWINGS**

FIG. 1 is a block diagram of the secure transaction system embodying the present invention, wherein a secure transaction server is part of a local area network, with the server being connected to the Internet and to the local area network via a firewall;

FIG. 2 is a functional block diagram of the secure transaction system embodying the present invention and illustrating the functional interaction of components of the system and a account holder;

FIG. 3 is a more detailed block diagram of the schema of the present invention;

FIG. 4 is a software block diagram illustrating the system architecture of the preferred embodiment in the web environment, also known as the secure transaction system;

FIG. 5 is a functional block diagram illustrating the structure and operation of the transaction clearinghouse database server process of the preferred embodiment;

FIG. 6 is a functional block illustrating the structure and operation of the transaction clearinghouse account holder authentication daemon of the preferred embodiment;

FIG. 7 is a block diagram illustrating the structure and operation of the transaction daemon of the preferred embodiment;

FIG. 8 is a functional block diagram illustrating the structure and operation of the transaction clearinghouse administration software of the preferred embodiment;

FIG. 9 is a functional block diagram illustrating the structure and operation of the server shared object of the preferred embodiment;

FIG. 10 is a functional block diagram illustrating the structure and operation of the server session manager of the preferred embodiment;

FIG. 11 is a functional block diagram illustrating the structure and operation of the server login common gateway interface (CGI) program of the preferred embodiment;

FIG. 12 is a functional block diagram illustrating the structure and operation of the server re-authentication common gateway interface (CGI) program of the preferred embodiment;

FIG. 13 is a functional block diagram illustrating the structure and operation of the server online application and activation common gateway interface (CGI) program of the preferred embodiment;

FIG. 14 is a functional block diagram illustrating the structure and operation of the server site administration common gateway interface program of the preferred embodiment;

FIG. 15 is a flow chart of the operation of the system at the start of a session where a account holder requests access to a secure transaction;

FIG. 16 is a flow chart of the system illustrating the steps that are taken during the login, account holder authentication and session initiation;

FIG. 17 is a flow chart of the sequence of steps that occur during transaction service and login;

FIG. 18 is a flow chart of the sequence of steps taken during a re-authentication operation;

FIG. 19 is a flow chart of the sequence of steps that occur during a session renewal;

FIG. 20 is a flow chart of the sequence of steps that occur during a session termination;

FIG. 21 is a block diagram of the hardware token access device that is part of the preferred embodiment of the present invention;

FIG. 22 is a block diagram of the magnetic card reader access device and access media that is part of the preferred embodiment of the present invention;

FIG. 23 is a block diagram of the smart card reader access device and access media that is part of the preferred embodiment of the present invention;

FIG. 24 is a block diagram of the biometric identification reader access device and access media that is part of the preferred embodiment of the present invention;

FIG. 25 is a block diagram of the secure central processing unit (CPU) access device and access media that is part of the preferred embodiment of the present invention;

FIG. 26 is a functional block diagram which illustrates multiple system servers with a single system transaction clearinghouse; and

FIG. 27 is a functional block diagram illustrating a system having multiple system servers and multiple system transaction clearinghouses.

#### DETAILED DESCRIPTION OF THE PREFERRED EMBODIMENT

Broadly stated, the present invention is directed to a secure transaction system that is particularly adapted for use with an untrusted network, such as the Internet worldwide web. As used herein, an untrusted network is defined as a public network with no controlling organization, with the path to access the network being undefined and the user being anonymous. A client-server application running over such a network has no control over the transmitted information during all the phases of transmission. The present invention provides a platform for securing transactions between consumers and suppliers on an untrusted network. Because of its superior design and operation, it is capable of operating servers and transaction clearinghouses in a geographically distributed fashion. The present invention implements its platform by restricting transaction services to only authenticated and authorized account holders and by tracking their transaction in a generic transaction model that can be easily integrated to any billing model.

The system has four major components as shown in FIG. 1, which are a transaction clearinghouse, indicated generally at 30; account holder administration software, shown generally

at 32; a secure transaction server, indicated generally at 34; and a number of account holder software, one of which is shown generally at 36. The account holders are connected to the Internet 38 via a modem connection or a similar means, and the Internet 38 has a connection to the server. The server 34 is connected to a local area network (LAN) 40 through a firewall computer 42. A firewall is used to separate a local area network from the outside world. In general, a local area network is connected to the outside world by a "gateway" computer. This gateway machine can be converted into a firewall by installing special software that does not let unauthorized TCP/IP packets passed from inside to outside and vice versa. The LAN 40 also provides a connection to the account holder administration software 32 and to the transaction clearinghouse 30. While the configuration shown in FIG. 1 has a single secure transaction server 34 and a single transaction clearinghouse server 30, the secure transaction system of the present invention is adapted to be used in other configurations, which may include multiple secure transaction servers being controlled by a single transaction clearinghouse 30 or multiple secure transaction servers that interact with multiple transaction clearinghouses 30. Such flexibility in configurations is an extremely desirable aspect of the present invention.

With respect to the major components of the system as shown in FIG. 1, the transaction clearinghouse 30 preferably resides on a back office platform in a corporate network. It has a secure interface to communicate with the secure transaction servers 34, which reside on the same machine that hosts the web server. The account holder software, on the other hand, resides on the account holder's desktop machine. The transaction clearinghouse server is preferably a Sun UNIX server which runs the transaction clearinghouse server processes and the database server. However, the database server could reside on a separate machine. The transaction clearinghouse is the entity that hosts all of the account and transaction data. The transaction clearinghouse provides a secure interface to the secure transaction servers 34, which enables the secure transaction servers 34 to authenticate the account holders and to send account holders' transaction data to the transaction clearinghouse. The transaction clearinghouse consists of a structured query language (SQL) database, which hosts the transaction clearinghouse database as well as an account holder authentication server for authenticating account holders on behalf of the secure transaction servers and processes online applications. The transaction clearinghouse also includes a transaction server that collects transaction data from the secure transaction servers 34 and updates the transaction clearinghouse database. The transaction clearinghouse also includes administration software 32 that provides a thin client graphical user interface to administer the transaction clearinghouse database.

With respect to the transaction clearinghouse administration software 32, it preferably resides on a desktop PC with a browser and is connected to the LAN 40 so that it can communicate with the transaction clearinghouse database server 30. This software will typically be on the LAN 40 of the organization so that database access through the administration software 32 is restricted within the organization. Using this administration software, an administrator can define the configuration for the account holder services, administer accounts, demographic data and transaction data. In the present invention, it is contemplated that the demographic data can be personal profile information, which may include at least two of the following items of information including: e-mail address, username, password, personal identification number, billing name, billing address, billing city, billing

state, billing zip code, billing country, shipping name, shipping address, shipping city, shipping state, shipping zip code, shipping country, shipping method, home phone number, work phone number, cellular phone number, facsimile phone number, credit card number, credit card expiration date, credit card type, debit card number, debit card expiration date, debit card type, card-holders name, date of birth, and social security number.

With respect to the secure transaction server 34, the software for it is preferably located on the same machine that hosts the web server. It is preferably a Sun Solaris machine or comparable computer. The secure transaction server 34 operates in conjunction with the transaction clearinghouse to authenticate and authorize account holders and to collect their transaction data. The secure transaction server 34 also interacts with the account holder software at the account holder computer 36 to provide transaction capture. The secure transaction server 34 consists of a shared object that is incorporated as a part of the web server software. It also has a collection of common gateway interface programs (CGI's) that implement authentication tasks, such as login and access device polling. A session manager is provided for building sessions for every valid account holder so that a transaction list that contains all of the tasks performed during a account holder's session can be kept. The server also includes a thin client site administration software program that provides a web based visual interface to administer the session manager and maintain account holder profiles. The server sends transaction data to the transaction clearinghouse at the end of every account holder's session and includes added functionality for processing and activating online account applications.

The account holder computer 36 includes software that enables an account holder's web browser to access the untrusted network. The account holder desktop PC contains a browser to access the untrusted network and also includes account holder software for enabling the account holder to access secure transaction services. The account holder software, in addition to enabling the access to a web site providing secure transaction services, also allows for enforcement of the login process, re-authentication process and transaction tracking. All of these features are controlled by the secure transaction server 34, which sends specific commands to the account holder software 36 to perform the tasks as needed. The account holder software is a plug-in or control that adds secure transaction functionality to standard browser software. The account holder also includes a hardware key for providing two or three factor authentication. FIGS. 21-25 illustrate the hardware key, which include a hardware token, magnetic card reader, smart card reader, or biometric identification reader connected to each account holder's client computer or alternatively a secure central processing unit as part of the account holder's client computer capable of reading access media that generates a unique digital ID.

The account holder access components preferably use the transmission control protocol/internet protocol (TCP/IP) and transaction datagram protocol/internet protocol (UDP/IP) to communicate with each other. Any communication that needs to go through the web server or the web browser will follow the hyper text transfer protocol (HTTP) which is based on TCP/IP. These protocols are well known to those skilled in the art. The account holder's PC accesses web sites using HTTP. The web server and secure transaction server 34 communicate with each other using UDP/IP. The secure transaction server 34 and the transaction clearinghouse 30 preferably communicate with each other using TCP/IP and the transaction clearinghouse servers communicate with a database using open database connectivity (ODBC) drivers most com-

monly over a TCP/IP network. The transaction clearinghouse administration software 32 communicates with the database using an ODBC driver, most commonly over a TCP/IP or IPX network.

5 The four main components of the preferred embodiment of the system as described with respect to FIG. 1 interact with one another using a distributed architecture which establishes a many-to-many relationship between the secure transaction servers 34 and the transaction clearinghouse 30. One transaction clearinghouse 30 can be monitoring multiple secure transaction servers 34 while each secure transaction server is interacting with multiple account holders 36. Similarly, a secure transaction server 34 can be configured to interact with multiple transaction clearinghouses 30.

10 The manner in which the preferred embodiment of the system operates in the web environment can be broadly seen by the functional block diagram of FIG. 2, which shows the transaction clearinghouse server 30, secure transaction server 34, and account holder 36 with steps that are taken during a session. The first step is for the account holder software 36 to request transaction services and that request is communicated to the secure transaction server 34 that then commands the account holder to login. The account holder software 36 inputs the login parameters that the secure transaction server 34 then forwards to the transaction clearinghouse. If the parameters are valid, the transaction clearinghouse 30 provides a response to the secure transaction server 34 that then enables the account holder software 36 to access the transaction services. The session transaction data is eventually forwarded for storage by the transaction clearinghouse 30.

15 While the steps that have been described with respect to FIG. 2 are a very broad overview of the preferred embodiment, the functional block diagram of FIG. 3 provides a more detailed general schema of the present invention. The system includes a server application 44, an account holder or client application 46, both of which are connected to an untrusted network via a traditional communication path indicated by the dotted lines 48 and 50. The system includes a session manager 52 for interacting with the transaction clearinghouse 30 and the secure transaction server 34 and a hardware key 54 which is connected to the account holder software 36. The solid lines connecting the blocks of the numbered components of FIG. 3 represent secure communications whereas the dotted lines are conventional communication paths that may not be secure.

20 Rather than describe the functions of the blocks of FIG. 3, the manner in which these components function will be described in connection with FIGS. 17-23, which provide more detailed flowcharts that relate to specific operations of the system.

25 The manner in which the system translates into the preferred embodiment in the web environment will be described in connection with the functional block diagram illustrated in FIG. 4. The transaction clearinghouse 30 contains the account and transaction database storage capability. The transaction clearinghouse 30 controls the authentication and authorization of account holders for individually enabled secure transaction web servers. The transaction clearinghouse 30 includes a number of subcomponents, including a transaction clearinghouse database server 56 that provides an open database connectivity (ODBC) interface to a structured query language (SQL) database that contains the account holder database and transaction data warehouse.

30 The transaction clearinghouse 30 also has an account holder authentication daemon 58 that processes the requests for account holder authentication by the secure transaction servers 34. A daemon 58 is a program that is not invoked

explicitly, but lays dormant waiting for one or more necessary conditions to occur such as an incoming request from one of its client programs. For every account holder authentication request, the account holder authentication daemon **58** first insures it is communicating with an authentic secure transaction server **34**, and then it queries the transaction clearinghouse database server **56** to find the account holder's information. Based on this information, it sends an authentication response back to the secure transaction server **34**. The account holder authentication daemon **58** also processes the secure transaction server's request for an online account holder application and an online account holder activation.

The transaction clearinghouse **30** also includes a transaction daemon **60** that is an independent server process that processes transaction data update requests made by secure transaction servers **34**. Similar to the account holder authentication daemon **58**, the transaction daemon **60** authenticates secure transaction servers before processing their requests. Upon successful authentication, it will accept all of the transaction data sent by a server and update the transaction clearinghouse database **56** with it. The transaction daemon **60** also authenticates secure transaction servers **34** before processing their request. The transaction clearinghouse **30** has administration software **64** that provides a visual interface on a computer with a web browser to administer the transaction clearinghouse database **56**.

With respect to the secure transaction server **34**, it runs in conjunction with a web server and is able to provide secure transaction services using the system of the present invention. The secure transaction server **34** authorizes each web transaction that involves account holder access of transaction services and does so by communicating with the account holder software **36** to make the account holders login. If the login is successful, the secure transaction server **34** initiates a session and collects all transaction data so that at the end of a session it can send the transaction data to the transaction clearinghouse. The secure transaction server also provides the functionality of session re-authentication. The secure transaction server includes a number of subcomponents including the session manager **52** which is a server process that processes messages sent by an account holder access shared object **66**, an account holder access common gateway interface programs (CGI's) **68** and the transaction clearinghouse **30**.

When an account holder **36** tries to log into a secure transaction system enabled web site, the session manager **52** communicates with the transaction clearinghouse **30** to authenticate the account holder. If successful, the session manager will start a new session for the account holder and from that point on, the account holder can access transaction services. Each web transaction during the session is reported to the session manager by the shared object **66** so that the session manager **52** can build a list of transactions for the account holder. At the end of the session, the session manager will send all of the session data and transaction data to the transaction clearinghouse **30** to update the database. If the system is utilizing two or three factor authentication (e.g., the user-name, password, PIN plus the digital ID generated by the access media read by the hardware key attached to the account holder's computer), the session manager **52** periodically communicates with the shared object **66** to perform re-authentication which involves polling of the account holder software **36** to insure that the hardware key **54** continues to be attached to the account holder computer.

The server shared object **66** is a binary module which provides function pointers to a web server **69** to perform secure transaction server **34** specific operations. To enable this, the server configuration files need to be changed so that

the web server **69** knows which transaction services are provided by the secure transaction system. In this way, whenever an account holder attempts to access a transaction service, the server will call upon the account holder access functions that are defined in the shared object **66** and the web server **69** will not process the request for transaction services until it receives permission to do so from these functions. The functions in the shared object **66** insure that the account holder is operating as a valid session. If it is not a valid session, the functions redirect the account holder to the login process so that a new session can be created for the account holder. Once there is an active session, the shared object **66** will grant permission to the web server **69** to process requests for transaction services and once the request has been processed, the shared object sends a message to the session manager **52** about a particular transaction so that the session manager can update its lists of transactions for the active session.

There are a number of account holder access common gateway interface programs (CGI's) that are a part of the secure transaction server **34**, including a login CGI **68**. Any time an account holder is redirected by the system shared object **66** to login and start a new session, the login CGI gets executed. These CGI's communicate with the account holder software to authenticate the secure transaction server and send a command to force the account holder to login. When the CGI's get the login parameters sent by the account holder software **36**, they send a request to the session manager **52** to authenticate the account holder and start a new session. There is also a re-authentication CGI **70** that is provided. Once a session has been initiated, periodically the shared object **66** will redirect the account holder to get re-authenticated. The re-authentication CGI **70** communicates with the account holder software **36** to poll the account holder's machine for the hardware key **54**, and based upon the response, the re-authentication CGI's communicates with the session manager **52** to validate re-authentication and renew the account holder session.

The secure transaction server **34** also includes an online account holder application and activation CGI's **74** which allow a person to apply online for transaction services. The CGI's collect the application data and send it to the transaction clearinghouse **30** that updates the account holder access database. Also, for an existing account holder who is trying to apply for another account, the CGI's will communicate with the transaction clearinghouse to get the account data on the account holder in order to fill out as much of the application automatically as it can. The activation feature is for users who have been approved and are trying to access secure transaction services for the first time. The CGI's for activation insure that the account holder has properly installed the account holder software and then these CGI's will send a message to the transaction clearinghouse to activate the account holder so that these approved users can access the new service. A site administration CGI **76** is another component included for providing an HTML visual interface to define the account holder profile and administer the session manager **52** for that particular account holder profile.

The account holder software **36** is installed on the account holder's personal computer. This software enables a web browser **77** to access the transaction services **78** provided by the secure transaction server. The account holder software is a plug-in or control that adds secure transaction functionality **79** to standard browser software. The account holder software accepts messages from the web server **69** and takes actions as commanded by the secure transaction server such as making the account holder login, polling for the optional hardware key, encrypting the login parameters and sending it to the

secure transaction server. The account holder software also authenticates the server 34 before accepting any commands from it so that only authenticate servers can command the account holder software.

Referring to FIG. 5, the main function of the transaction clearinghouse database server 56 is to provide the database interface to the rest of the account holder access components. The transaction clearinghouse database server 56 contains the enterprise-wide account holder and transaction data warehouse. This database server is a SQL server that has an ODBC interface so that the clients can interact with it using ODBC. The processes and application that interact directly with the transaction clearinghouse database server 56 are the account holder authentication daemon 58, the transaction daemon 60, and the thin client transaction clearinghouse administration software 64.

Referring to FIG. 6, the account holder authentication daemon 58 interacts with the transaction clearinghouse database server 56, the session manager 52, the account holder application and activation CGI's 74, and any CGI's that use the API's provided by the secure transaction system, such as the credit card processing CGI's 80. In order to start a new session for a account holder, the session manager 52 sends an authenticate login (AL) message to the account holder authentication daemon 58, which queries the transaction clearinghouse database server 56 to find the appropriate account holder records in order to do the login validation. The result of this validation is sent back to the session manager 52 as an authentication response (AR) message.

The online application CGI's 74 interact with the account holder authentication daemon 58 to process an online account holder application. Normally, users fill out an online application form and submit it to one of the online application CGI's which will send all the application data in the form of an application (AP) message to the account holder authentication daemon. The daemon will verify and update the database with the application information and send back an application response (PR) message to the application CGI's indicating the status of the database update.

In cases where an existing account holder is applying for another account, the application CGI's 74 communicate with the account holder authentication daemon 58 to get the account holder information on the current account holder so that the application form can be filled automatically. In order to do this, one of the application CGI's 74 sends a verify application (VA) message to the account holder authentication daemon 58. The daemon will query the transaction clearinghouse database server 64 to verify the applicant and get the account holder information. Based on the query results, it will send a verification response (VR) back to the application CGI 74 which will contain the account holder information. The application CGI 74 will fill out the account holder part of the application form with this information. The account holder fills out the rest and submits the form that gets processed through the AP/PR message mentioned previously.

Once a user has been approved, the user needs to activate the account in order to access transaction services. This can be done online through the online activation CGI's 74. Typically, an approved user (i.e., an account holder) will have to login in order to access the online activation CGI 74, which in turn sends an AA (Activate Applicant) message to the account holder authentication daemon 58 with the approved user's login parameters. The daemon 58 will query the transaction clearinghouse database server 64 to validate this information, and based on the validation results, it will send back an activation response (AR) message to the online activation CGI.

For web applications that need credit card information on account holders, the account holder authentication daemon 58 provides an API to do so. This also assumes that the account holder has logged in successfully and has an active session, which means these web applications need to be secured. In order to obtain the credit card information, these web applications can send a CC (credit card) message to the account holder authentication daemon 58. The daemon will first validate the account holder and if the validation is successful, it will send back a credit response (CR) to the credit card processing web application 78 that includes the account holder's credit card information.

Referring to FIG. 7, the main task of the transaction daemon 60 is to update the transaction clearinghouse database server 56 with transaction data sent by the secure transaction server session manager 52. The transaction daemon 60 is an independent process listening for TCP requests on a specific, well-known TCP port. When a account holder session terminates, the session manager 52 will send a transaction session (US) message to the transaction daemon 60 that provides some generic information about the account holder's session and also the number of transactions in the session. This message is followed by a series of session transaction (ST) messages, where each transaction in that session is represented by a ST message. The transaction daemon 60 reads the US message and the following ST message(s), formulates SQL queries that will update all that data into the transaction clearinghouse database 56. The transaction daemon 60 will then send back a message confirmation (MC) back to the session manager 52 that indicates the status of the database update.

As shown in FIG. 8, the transaction clearinghouse administration software 64 is a thin client GUI web-based application for transaction clearinghouse database administration. This software runs on a computer with a web browser and communicates with the transaction clearinghouse database server 56. This application will typically be on the private network of an organization so that database access through the administration software 64 is restricted within the organization. The administration software 64 allows an administrator to define the particular transaction services that can be accessed by an account holder. It allows entering users as an account holder, approving and activating the account holder, and maintaining account holder profiles. It also provides inquiry screens to peruse transaction data. Also provided are table maintenance screens for the code tables in the database. The transaction clearinghouse servers preferably communicate with a database using open database connectivity (ODBC) drivers 81 most commonly over a TCP/IP network, and the transaction clearinghouse administration software 32 communicates with the database using an ODBC driver 81, most commonly over a TCP/IP or IPX network. As shown in FIG. 9, the account holder access shared object 66 is a binary module that combines with the web server 69 to provide system-specific function pointers to the web server. Thus, when the web server 69 is configured to protect transaction services using the system, it will call upon these system specific functions. These functions provide a variety of features ranging from redirecting an account holder to the login CGI's 68 to communicating with the session manager 52 to authenticate every request for transaction services. Whenever there is an incoming request from a web browser 77 including the account holder software 36 that attempts to access a transaction service, the web server 69 invokes the shared object 66. The shared object 66 calls a secure transaction system function that first looks for an active session ID in the HTTP headers. If it does not find the session ID, it will redirect the account holder to the login CGI's 68 in order to

**11**

initiate the login process. If it finds a session ID, it sends a check session (CS) message to the session manager **52** to validate the session ID. The session manager **52** will send the results of its validation in a session response (SR) message.

If the SR message has a SUCCESS status, the shared object **66** grants permission to the web server **69** to process the request for the account holder to access transaction services. At the end of processing this request, the shared object **66** calls another secure transaction system function that sends an end transaction (ET) message to the session manager so that the session manager **52** can log the end time for the specific web transaction. Periodically, the SR message will ask the shared object **66** to perform session re-authentication. At such times, the shared object **66** redirects the account holder to re-authentication CGI's **70**.

With the system architecture, transactions are protected on a directory level. A web master or a system administrator needs to determine which transactions are to be protected and make sure that all these transactions are organized in separate directories from unprotected transaction services. In this way, the web server configuration can be changed to protect these particular directories using the secure transaction system. Among other things, the configuration parameters also need to state where the session manager **52** is running and the port where it is listening for UDP requests. If there are multiple account holders being hosted from the same web servers **69**, it is very important to have their transaction services contained in separate directories, and also very important is to have separate copies of session managers **52** running for each account holder. This ensures that account holder authentication, authorization, and transaction tracking is done separately for separate account holders.

The secure transaction server session manager shown in FIG. 10 is an independent server process. It starts by reading configuration parameters from its configuration file, sessiond.conf. It listens for requests on two different ports—one UDP, and one TCP. The UDP port communicates with the account holder access shared object **66** and the account holder access CGI's that reside on the same machine where the session manager **52** is running. The TCP port is for communication with the account holder access transaction clearinghouse daemons.

The session manager **52** maintains a binary tree list of all the active account holder sessions. For every session, it maintains a linked list of all the transactions for that session. As stated in the description of the shared object **66**, every time a web request comes in for a transaction service, the web server **69** will invoke the shared object **66**. The shared object **66** looks at the web server configuration files to determine which session manager **52** (hostname and UDP port number) to send its check session (CS) message. In processing a CS message, the session manager **52** will traverse its list of active sessions looking for the particular session ID, and sends the result of this search back in a session response (SR) message.

During login, the login CGI's **68** send an initiate session (IS) message to the session manager **52**, which will read the login parameters, and send an authenticate login (AL) message to the transaction clearinghouse account holder authentication daemon **58**. The session manager **52** will read the account holder authentication daemon's **58** authentication response (AR) and determine whether or not to create a new session entry, and sends a session response (SR) back to the login CGI's **68** indicating the result of the session initiation process.

While processing a CS message sent by the shared object **66**, periodically the session manager **52** will find that a particular session needs to be re-authenticated. In such instances,

**12**

the session manager **52** will respond back to the shared object **66** with a session response (SR) message that tells the shared object **66** to initiate the re-authentication process. The shared object **66** in turn invokes the re-authentication CGI's **70**. The re-authentication CGI's **70** perform the re-authentication task with the account holder software **36**, and sends the results in a renew session (RS) message to the session manager **52**. The RS message contains the newly encrypted digital ID optionally stored on the access media which is read by the hardware key **54** attached to the account holder's machine. The session manager **52** authenticates the digital ID by comparing it to the information it has in the session entry for the particular account holder. The results of this authentication are sent back to the re-authentication CGI **70** in a session response (SR) message.

During specific time intervals as set in the session manager **52** configuration, the session manager goes through its list of sessions and times out any idle sessions, flagging them as inactive. These are sessions that have not had an activity in the last n seconds, where n is a session manager configuration (REFRESH\_TIME) value. For each one of these inactive sessions, the session manager **52** initiates a process that will send all the transaction data collected for that session to the transaction clearinghouse's transaction daemon **60**. The process first reads the session-entry and sends a transaction session (US) message that will tell the transaction daemon **60** how many transaction entries will be sent for that session. The US message is followed by a series of session transaction (ST) messages where each ST message represents a transaction for that session. The process terminates after sending all the US and ST messages. The transaction daemon **60** will update the transaction clearinghouse database with all the transaction data, and sends a message confirmation (MC) message back to the session manager **52**. The session manager **52** determines which specific session the MC message is for, and deletes that session and its transactions from its list. If the MC message status is not successful, the session manager **52** tries to resend the transaction data. The number of retries is set in the session manager **52** configuration. If it is still unsuccessful, then the session manager **52** sends an e-mail to the system administrator indicating the error in transaction data update.

Another entity that the session manager **52** performs processing for is the site administration CGI's **76**. The specific operations provided are data recovery, data dump, and data restore features. During data recovery, the site administration CGI's **76** send a DR (data recovery) message to the session manager **52**. The session manager **52** will retry sending the transaction data for the session(s) specified in the DR message to the transaction clearinghouse's transaction daemon **60**.

During a data dump, the site administration CGI **76** sends a data dump (DD) message to the session manager **52** who makes a copy of all the active session data into a flat text file under the filename specified in the DD message. During a restore dump, the site administration CGI **76** sends a restore dump (RD) message to the session manager **52** who reads the dump file as named in the RD message and builds its list of sessions and transactions from the dump file data. To all these messages (DR, DD, RD), the session manager **52** sends a SR message back to the site administration CGI's **76** indicating the results of the particular operations whether they were successful or not.

Referring to FIG. 11, the login CGI's **68** is initiated when the shared object **66** redirects a account holder to login. It first sends a start login message to the account holder software **36** combined with the web browser **77** through the web server **69**.

13

The account holder software 36 then creates a random challenge and sends it to the login CGI's 68 for secure transaction server authentication purposes. The login CGI's 68 encrypts the secure transaction server's password using the challenge sent by the account holder software 36 and sends it back to the account holder software along with a login command and a new random challenge created by the login CGI 68. The account holder software 36 then authenticates the secure transaction server's password, and if it authenticates successfully, it will force the account holder to login. The login parameters obtained from the account holder and the hardware key 54 are encrypted using the challenge sent by the login CGI 68, and sent back to the login CGI.

The login CGI's 68 take the encrypted login parameters sent by the account holder software 36 and send an initiate session (IS) message to the session manager 52. The session manager 52 conducts the account holder verification with the aid of the transaction clearinghouse 30 and sends back a session response (SR) indicating if a new session entry was created. If SR status is successful, the login CGI 68 will put the session ID in the HTTP headers for re-authentication purposes.

As shown in FIG. 12, the re-authentication CGI's 70 are invoked by the account holder access shared object 66. The web server 69 sends a check login message to the account holder software 36 combined with the web browser 77 with a newly created challenge. In response to this message, the account holder software 36 polls the hardware key 54, reads the digital ID from the access media, and encrypts it using the challenge sent by the re-authentication CGI's 70, which is sent back to the re-authentication CGI 70 who will validate the information by sending a renew session (RS) message to the session manager 52. The session manager 52 validates the encrypted digital ID and sends back a session response (SR) message indicating the status of the re-authentication. If SR status is successful, the re-authentication CGI 70 redirects the account holder to the protected transaction services, otherwise they are directed to the login process.

Referring to FIG. 13, the online application process is initiated by a new user filling out an HTML application form and submitting it to the application CGI 74. If the user is an existing account holder, a separate link can be activated by the user that will automatically fill out the demographic part of the application form. When an existing account holder goes through this link, the account holder must login. The particular application CGI 74 will then send a verify application (VA) message to the account holder authentication daemon 58. The daemon 58 will first authenticate the account holder, and if the authentication is successful, it will send back the demographic information on the account holder in its verification response (VR) message. The application CGI 74 will fill out the HTML application form with the information in the VR message. For a user who is not an existing account holder, the user is required to go to the application form directly to manually fill out all the fields, and submit the form back to the web server 69.

When the application form is submitted to the web server 69, the application data is sent to another application CGI 74 who will send an application (AP) message to the account holder authentication daemon 58. The daemon 58 will verify all the application data and update the transaction clearinghouse database. The result of the database update is sent back to the application CGI 74 in an application response (PR) message. The application CGI 74 will then display the result of this process to the user on the web browser 77.

The application approval process can be conducted in a variety of ways. For account holders offering one-factor

14

authentication only, where a hardware key 54 is not used, a user can be instantly approved during the time of application, in which case the PR message contains the username, password, PIN assigned to the user. This information is immediately displayed back to the user so that the user can quickly proceed with the account holder activation process. Alternatively, another method is not approving the application immediately. Instead, a system administrator will perform additional processing of the application data to ensure that the user meets all the prerequisites of being an account holder. This could involve things like collecting payment, credit checks, etc. Once the requirements are met, the system administrator can approve the user using the transaction clearinghouse administration application software.

The result of the application approval process is that the user will now be assigned a unique account username and a password. If the account holder uses two-factor authentication, the approval process also involves assigning a unique digital ID to the user, and microcoding that digital ID into the access media read by the hardware key 54. All this information (username, password, PIN, digital ID), the user's hardware key and access media 54, and the account holder software 36 need to be made available to the approved user so that the user can successfully install the hardware key and account holder software 36 on the desktop, and proceed with the activation process.

The activation process is complete when the user becomes an account holder for a particular set of transaction services. Similar to the application process, this can be done through either online or through the account holder administration software 32. Online activation requires an approved user to install the account holder software on their desktop and visit the activation URL using the web browser 77. When the user clicks on the activation URL, the user must login. At this point, the approved user will use the username, password, PIN and the hardware key when using a two-factor authentication login. The activation CGI 74 takes all this information and sends an approve user (AU) message to the transaction clearinghouse's account holder authentication daemon 58. This daemon 58 will accept the AU message, and verify all the information with the approved user's information in the transaction clearinghouse database. If the verification is successful, the account holder authentication daemon 58 will create a new account holder record for the user if there is not already one, and also create a new account holder record for the particular account holder(s) for which the user was approved for. The result of this process is sent back to the activation CGI in an activation response (RA) message. If RA message status is successful, the activation CGI 74 will display a successful activation message to the account holder, and give the account holder an option to change their password if desired. Otherwise, the activation CGI 74 will display the error message explaining why application activation could not be conducted successfully.

A feature of the online application and activation process is the password change feature that can be made available as a separate link in a secured web site. This link must be protected by the system so that only valid account holders can use this feature. When this link is accessed, a password/PIN change form is displayed to the account holder where they type in the old and new passwords/PINs. Once this form is submitted, a password/PIN change CGI 82 will send a change password/PIN (CP) message to the account holder authentication daemon 58 in the transaction clearinghouse that will verify the account holder and the old password/PIN. If the verification is successful, the account holder authentication daemon 58 will make the password/PIN change in the transaction clearing-

15

house database. The status of this process is sent back to the password change CGI 82 in a password/PIN response (RP) response. Based on the RP message status, the password/PIN change CGI will display a message to the account holder indicating whether the password/PIN change was carried out successfully.

As shown in FIG. 14, the site administration CGI's 76 allows for the session manager configuration entries to be defined and maintained through an HTML interface. It also allows for the starting, stopping, and restarting of the session manager(s) 52. The specific operations provided by the site administration CGI's 76 that involve message interaction with the session manager 52 are the data recovery, data dump, and the data restore features. During a data recovery, the site administration CGI's 76 send a DR (data recovery) message to the session manager 52. The session manager will retry sending the transaction data for the session(s) specified in the DR message to the transaction clearinghouse's transaction daemon 60.

During data dump, the site administration CGI 76 sends a data dump (DD) message to the session manager 52 that makes a copy of all the active session data into a flat text file under a specified filename in the DD message. During restore dump, the site administration CGI 76 sends a restore dump (RD) message to the session manager 52, which reads the named dump file(s) from the RD message and builds a list of sessions and transactions from the dump file data. For any of these messages (DR, DD, RD), the session manager 52 sends a SR message back to the site administration CGI's 76 for indicating the results of success or failure for these particular operations.

FIGS. 4-14 described the software components of the preferred embodiment. The specific operations of the system will now be described in connection with the flow charts of FIGS. 15-20. In order to distinguish the present invention from the preferred embodiment in the web environment, the flowcharts use different terminology for the system components. The following table provides a cross reference between the flowchart components and the preferred embodiment.

FLOWCHART COMPONENTS	REFERRED EMBODIMENT ONTO WEB ENVIRONMENT
Client Application	Web browser
Client Messenger	a module of account holder software
Server Authenticator	a module of account holder software
Log-in interface	a module of account holder software
Access device interface	a module of account holder software
Client Cryptographer	a module of account holder software
Content Controller	a module of account holder software
Network transaction tracker	a module of account holder software
Server Application	Web Server
Communication Headers	HTTP headers
Client Authenticator	a module of Shared Object for Web Server
Transaction Monitor	a module of Shared object for Web Server
Log-in Enforcer	Log-in CGI's
Access device Validator	Re-authentication CGI's
Session Validator	a module of Session Manager
Session Initiator	a module of Session Manager
Session Terminator	a module of Session Manager
Authentication Server	Transaction clearinghouse Account holder authentication daemon
Transaction Data Server	Transaction clearinghouse Transaction daemon

Referring to FIG. 15, the flow chart illustrating the sequence of steps that occur during the start of a session is illustrated and begins with the account holder requesting access to a transaction service (block 100). The server appli-

16

cation forwards the request to the client authenticator (block 102). If the session ID is in the communication headers (block 104), the client authenticator sends a check session message to the session validator (block 106), and the session validator searches for a session entry in its list of active sessions (block 108). If the session ID is not in the communication headers (block 104), the client authenticator denies permission to the server application for servicing the account holder's request (block 110). Also, if the active session entry is not found (block 112), the session validator sends an unsuccessful session response to the client authenticator (block 114). However, if there was an active session entry found, a subroutine of transaction service and logging is initiated (block 116), which will be described later in conjunction with FIG. 17. If the client authenticator, on the other hand, denies permission to the server application (block 110) when the session ID is in the communication header (block 104) or after the session validator sends an unsuccessful session response (block 114), the server application invokes the login enforcer to make the account holder login (block 117). This results in a start login message being sent to the client messenger through the client application (block 118). The client messenger then sends a random challenge to the login enforcer through the server application (block 120), and the login enforcer encrypts the server application password with a client messenger challenger (block 122). The login enforcer then sends a login command in its encrypted password to the client messenger with a new random challenge of its own (block 124), and the client messenger then invokes server authenticator to authenticate server applications password (block 126). If the server authentication is successful (block 128), another subroutine of a login, account holder authentication and session initiation process is initiated (block 130), which will be described in conjunction with FIG. 16. If not, the client messenger displays a server authentication error message to the account holder (block 132), and the process is completed.

A flow chart of the login, account holder authentication, and session initiation subroutine is shown in FIG. 16, and indicated generally at 103. The client messenger first invokes a login interface to prompt account holder for a username, a password, and/or a PIN (block 140). The account holder then enters the username, the password, and/or the PIN (block 142), followed by the login interface requesting the hardware key interface to poll for the hardware key (block 144). If using two or three factor authentication, the hardware key interface reads the digital ID from the access media and sends it to the login interface (block 146). In the case of one factor authentication, the login interface assigns a blank digital ID for the login parameters. The login interface then sends the login parameters, including the username, password and digital ID to the client cryptographer (block 148). The client cryptographer encrypts the password and the digital ID using the challenge sent by the login enforcer and sends them to the login enforcer (block 150). The login enforcer then sends an initiate session message to the session initiator with the encrypted login parameters (block 152). The session initiator accordingly sends an authenticate login message to the transaction clearinghouse account holder authentication server (block 154), and the account holder authentication server accesses the account holder's information from its database and authenticates the login parameters (block 156). If using two or three factor authentication, this authentication involves the comparison of the digital ID, otherwise only username, password, and PIN are considered as login parameters. If the authentication was successful (block 158), the account holder authentication server sends a successful authentication response message to the session initiator

(block 160). The session initiator enters a new session entry for the account holder in its list of active session with a unique session ID (block 162). The session initiator also sends a successful session response to the login enforcer (block 164), followed by the login enforcer entering the account holder's new session ID in the communication headers for re-authentication purposes (block 166). The login enforcer also grants permission to service the account holder's request for secure transaction services (block 168), and proceeds to initiate the subroutine of transaction service and logging (block 116) shown in FIG. 17. However, if authentication is unsuccessful (block 158), the account holder authentication server sends an unsuccessful authentication response to the session initiator (block 172). The session initiator then sends an unsuccessful session response to the login enforcer (block 174). The login enforcer accordingly denies permission to the server application to service the account holder's request for transaction services (block 176), and the server application sends back an error response to the account holder (block 178).

The subroutine of the transaction service and logging process (block 16) is shown in FIG. 17. The session validator first enters a new transaction entry for the account holder's current session (block 180). The session validator then sends a successful session response to the client authenticator (block 182), and the client authenticator grants permission to the server application to service the account holder's request (block 184). The server application invokes the appropriate service function to enable the account holder to access the requested transaction services (block 186) and the transaction monitor sends an end transaction message to the session validator (block 188). The session validator updates the transaction entry with the transaction-specific information in the end transaction message (block 190).

In accordance with an important aspect of the present invention, the system is preferably adapted to periodically re-authenticate an active session to prevent unauthorized use by someone who no longer has the hardware key 54 connected to his computer. With respect to the re-authentication process, and referring to FIG. 18, the process begins with an account holder in an active session requesting a transaction service (block 200). The server application forwards the request to the client authenticator (block 202), and communication headers are screened to see if they have a session ID (block 204). If there is no session ID (block 204), the client authenticator denies permission to the server application to service the request (block 206) and the server application directs the account holder to the login enforcer to start a new session (block 208). If, however, the session ID is in the communication header (block 204), the client authenticator sends a check session CS message to the session validator (block 210).

From the CS message, the session validator searches for a session entry in its list of active sessions (block 212) and determines whether an activate session entry was found (block 214). If not, the session validator sends an unsuccessful session response to the client authenticator (block 216) and the client authenticator denies permission to service the request (block 206). The server application would again direct the account holder to the login enforcer to start a new session (block 208). If an active session is found (block 214), then the session validator checks for the time of the last polling of the account holder's machine to determine whether the hardware key 54 is present (block 218). The time duration is checked to determine if the preset time limit has been exceeded (block 220), and if it has not, then the system goes to the subroutine of the transaction service and logging step (block 170) (see FIG. 17). If the time duration has exceeded

the preset time limit, the session validator sends a session response to the client authenticator asking to poll for the account holder's hardware key attached to the account holder's computer (block 222). The client authenticator invokes the access device validator (block 224), and the access device validator then sends the check login message to client messenger with a new randomly generated challenge (block 226). The client messenger invokes the login interface (block 228), which in turn invokes the access device key interface (block 230). The access device interface polls the account holder's machine for the hardware key 54 (block 232) and reads the digital ID from the access media. If the digital ID is successfully read (block 234), the program implements a session renewal (block 236), which is shown in FIG. 19. If the digital ID is not successfully read (block 234), the access device interface sends an error message to the login interface (block 238) and the login interface generates an error message to the client messenger (block 240). The client messenger then sends an unsuccessful polling message to the access device validator, which redirects the account holder to the login enforcer (block 242).

With respect to the session renewal and referring to FIG. 19, the access device interface reads the digital ID of the access media and submits it to the login interface (block 250), which in turn submits the digital ID to the client cryptographer (block 252). The client cryptographer encrypts the digital ID using the challenge sent by the access device validator and sends the encrypted digital ID 10 to the access device validator (block 254), which then sends a renew session message to the session validator with the encrypted digital ID (block 256). The session validator finds account holder session entry and validates the encrypted digital ID (block 258) and determines whether the validation was successful (block 260). If not (block 260), the session validator sends an unsuccessful session response to the access device validator (block 262), and the access device validator redirects the account holder to the login enforcer to start a new session (block 264). If validation was successful (block 260), the session validator updates the session entry's time of last re-authentication (block 266) and sends a successful session response to the access device validator (block 268). The access device validator grants permission to the server application to process the account holder's request for transaction services (block 270), and then proceeds to the transaction service and logging step (block 116) (see FIG. 17).

With respect to session termination and referring to FIG. 20, the first step is to begin with the first session entry of a session list (block 280) and the session terminator checks the difference between the current time and the time of the last request (block 282). If the time difference did not exceed the idle time limit (block 284), the program determines whether the first session entry is the last session entry in the session list (block 286). If so, the session is terminated (block 288). If it is not the last session entry in the list (block 286), the program fetches a next session entry in the list (block 288) and return to block 282. If the time difference did exceed the idle time limit (block 284), the session terminator tags the session entry as inactive (block 290) and sends all session transaction data to the transaction clearinghouse's transaction data server (block 292). The transaction data server updates the transaction clearinghouse database with the session transaction data (block 294), and the program determines whether the update was successful (block 296). If not, the transaction data server sends an unsuccessful message confirmation to the session terminator (block 298), which prompts the session terminator to send an error message to the system administrator (block 300). If the update was successful (block 296), the transaction

19

data server sends a successful message confirmation to the session terminator (block 302) and the session terminator then removes the session entry from the session list (block 304).

In accordance with another important aspect of the present invention, and referring to FIG. 21, a hardware token access device 450 for use as the hardware key 54 is shown in the illustrated functional block diagram. The access device 450 is an external hardware device, such as the iKey 1000 USB Smart Token device manufactured by Rainbow Technologies of Irvine, Calif. The hardware token access device 450 preferably connects to the USB port of the account holder's personal computer. The major function of the hardware token access device 450 is to uniquely identify a account holder that desires to access the transaction services and computer resources of an untrusted network, such as the Internet. It is used in conjunction with the username, password, and/or PIN to provide two factor authentication. Generally, two factor authentication provides that something is known (e.g., the username and password) and something is held (e.g., the physical hardware token that is attached to the computer or built into the computer). While the Rainbow iKey 1000 USB Smart Token is the preferred embodiment for the hardware token access device 450, it should be understood that the two factor authentication could be provided by some other physical device, such as a credit card, a key, an ATM card, or the like which is known to have been assigned and given to a specific person.

In FIG. 21, the hardware token access device 450 includes a port interface 480, which provides an interface to support the personal computer of the account holder 36. Such may include, for example, USB, parallel, serial and/or keyboard ports. The access device 450 is transparent to the personal computer interface being utilized and does not prohibit the personal computer interface from being used in a normal fashion. In the Rainbow iKey 1000 Smart Token, it is preferred that the hardware token be connected to the USB port. The hardware token also includes a data bus buffer 482, which provides a minimum internal data bus of eight bits regardless of the port interface configuration. A read/write control logic block 484 manages all the internal and external transfer of data controlled status, while a control register 486 initializes the functional configuration of the access device 450. A status register 488 contains the result of the last operation performed using the control register 486 on the read/write control logic 484. A message digest encryption 490 is used to encrypt both a nonvolatile general purpose memory 492 during memory read and password read operations. The message digest encryption engine 490 accepts a seed value from the port interface 480 that can be used to uniquely encrypt the data being read. The memory 492 contains a minimum of 1024 bytes of data that can be used for storage of information for personally identifying the account holder. This information can include, but is not limited to a digital certificate. A password register 494 accepts a minimum of a 64 bit password from the port interface 480, and a password comparator 496 performs a logical XOR on the contents of the password register in the contents of the nonvolatile password memory 492. When the contents of the password register 494 are equal to the contents of the nonvolatile password memory 498, several operations can be performed, such as reading the nonvolatile general purpose memory, read the encrypted nonvolatile password memory, writing the nonvolatile general purpose memory, writing the nonvolatile password memory and writing a seed value to the message digest encryption engine. The nonvolatile password memory contains a mini-

20

mum of a 64 bit password. The password is set to a known default value at the time of manufacture but can be reprogrammed at any time.

In accordance with another important aspect of the present invention, and referring to FIG. 22, a magnetic card reader access device in use with an access media 54 is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and indicated generally at 499. A magnetic card is a plastic card with a strip of magnetic recording tape adhered to the back of the card. The magnetic recording strip has three tracks that can be used for storing and retrieving data. In the context of the preferred embodiment, the magnetic card 500 is the preferred access media containing a digital ID. Magnetic stripe cards, which typically only store about 1 kilobyte of data (compared with 8, 16, or 32 KB in smart cards), do not have a CPU and rely on the card reader, the PC to which it's attached, or a remote computer accessed via modem to perform transaction processing. Magnetic card technology is widely utilized in Point of Sale (POS) terminals, Automated Teller Machines (ATM), ticketing, card issuing, transportation, and access control.

Two types of devices, a reader and a terminal can read magnetic cards. A reader is interfaced to a personal computer for the majority of its processing requirements, while a terminal is a self-contained processing device. Magnetic card readers are available that interface to RS232 serial ports, USB ports, PCMCIA slots, parallel ports, infrared IRDA ports and keyboards. Terminals have their own operating systems and in addition to reading a magnetic card typically support other functions such as network connectivity, transaction printing, and keypad entry. Both terminals and readers are considered access devices 501 in the context of the preferred embodiment:

For example, a magnetic card reader can be attached to a personal computer (PC) and serves the role of an access device. The magnetic card reader connects in-line between a PC and its keyboard. The magnetic card reader is intended to remain virtually invisible to both the PC and the keyboard until a magnetic card is read. When a magnetic card is read, the magnetic card reader takes over the interface to the PC and sends card data using the same scan codes used by the keyboard. These scan codes are routed to the account holder software 36. Magnetic card readers also support the operation of a keypad that can be used to enter one or any combination of username, password or PIN codes in addition to the digital ID read from the access media by the access device.

In accordance with another important aspect of the present invention, and referring to FIG. 23, a smart card reader access device in use with an access media is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and indicated generally at 502. A smart card is a type of plastic card embedded with a computer chip that stores and transacts data between users. This data can contain several digital IDs that are stored and processed within the card's chip, either a memory or a microprocessor. The card data is transacted via a reader that is part of a computing system. Smart cards greatly improve the convenience and security of any transaction. They provide tamper-proof storage of user and account identity. Smart cards protect against a full range of security threats, from careless storage of user passwords to sophisticated system hacks. Within the context of the preferred embodiment, a smart card 503 is considered access media.

Two types of devices, a reader and a terminal can read smart cards. A reader is interfaced to a personal computer for the majority of its processing requirements, while a terminal is a self-contained processing device. Both are considered

21

access devices in the context of the preferred embodiment. Both the terminals and the readers read and write to smart cards. Readers come in many forms and in a wide variety of capabilities. Smart card readers that interface to RS232 serial ports, USB ports, PCMCIA slots, floppy disk slots, parallel ports, infrared IRDA ports and keyboards are presently available. Smart card terminals have their own operating systems and typically support other functions such as reading a magnetic card, network connectivity, transaction printing, and keypad entry. Both the terminals and the readers are considered access devices 504 in the context of the preferred embodiment.

Smart cards have the tremendous advantage, over their magnetic stripe ancestors, of being able to execute cryptographic algorithms locally in their internal circuitry. This means that the user's secrets (be these PIN codes or keys) never have to leave the boundaries of the tamper-resistant silicon chip, thus bringing maximum security to the overall system where the cards are used. Smart-cards contain special-purpose microcontrollers with built-in self-programmable memory and tamper-resistant features intended to make the cost of a malevolent attack more than any benefits gained from the attack. Smart Card readers can also support the operation of a keypad that can be used to enter one or any combination of username, password or PIN codes in addition to the digital ID read from the access media by the access device.

In accordance with another important aspect of the present invention, and referring to FIG. 24, a biometric identification reader access device in use with an access media is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and generally indicated 505. As organizations search for more secure authentication methods for user access, e-commerce, and other security applications, biometrics is increasingly gaining attention in the marketplace. A biometric is one of the most secure and convenient authentication tool. It cannot be borrowed, stolen, or forgotten and is practically impossible to forge. Biometrics measure an individuals' unique physical or behavioral characteristics as a way to recognize or authenticate their identity. Common physical biometrics include fingerprints; hand or palm geometry; and retina, iris, or facial characteristics. Behavioral characters include signature, voice (which also has a physical component), keystroke pattern, and gait.

A biometric system works by capturing the chosen biometric with a biometric reader. The reader converts the biometric into a digital identification that is stored in a local repository for comparison during authentication. In the case of the preferred embodiment, the biometric reader 506 is equivalent to the access device; the biometric identification data 507 is equivalent to the digital ID created when the access device reads the fingerprint 508 access media; and the local repository that stores the biometric identification data can be the transaction clearinghouse. When logging into the secure transaction system, the account holder would have the chosen biometric (e.g., access media—fingerprint, palm, etc.) scanned by the biometric reader 506, forwarded to the clearinghouse using the previously described log-in process (FIGS. 15-20). The digital ID created by the biometric data would be compared to the digital ID already stored in the transaction clearinghouse for authenticity. It is also possible in the preferred embodiment to combine the digital ID created by the biometric scan to be supplemented with one or any combination of username, password, or PIN in addition to the digital ID read from the access media by the access device. Biometric identification can be also combined with smart cards or magnetic cards in the preferred embodiment.

22

In accordance with another important aspect of the present invention, and referring to FIG. 25, a secure central processing unit (CPU) in use with an access media is implemented as the hardware key 54 is shown in the illustrated functional block diagram, and indicated generally at 509. In order to secure the CPU, a trusted subsystem must be inserted into the standard personal computer platform. The trusted subsystem is then able to extend its trust to other parts of the whole platform by building a 'chain of trust' where each link extends its trust to the next one. In this way, the secure CPU subsystem provides the foundation for a fully trusted platform and a basis for extending trusted computing across system and network boundaries.

The root of trust is a small hardware device called a Trusted Platform Module (TPM) 510. The TPM 510 is basically a secure controller that provides features like secure memory, cryptographic sign/verify, and an immutable key pair used to generate anonymous identities. In the preferred embodiment, the CPU and its associated platform 511 is the access device and the secure memory of the TPM 510 preferably acts as the access media and holds several types of unique digital IDs. Together they provide secure CPU functionality and provide all the functions of the account holder's PC. Another important feature of the TPM 510 is the possibility of producing random numbers. The TPM 510 can create digital signatures using the random number generator as the source of randomness required by the digital ID generation process. In order to generate a unique digital ID, each single TPM 510 has a unique key that identifies the TPM.

With these capabilities, the TPM 510 is able to produce a statistically unique digital fingerprint of the PC's basic input/output system (BIOS) firmware at boot time. This fingerprint is also called an integrity metric or cryptographic digest. Once this metric is available, it is saved in the TPM's secure memory location. During the PC boot process, other integrity metrics are collected from the PC platform, for instance, fingerprints of the boot loader and the operating system itself. Device drivers may be hashed; even hardware like PCI cards can be detected and identified. Every metric of the TPM 510 is concatenated to the already available metrics. This generates a final metric, which provides a unique digital ID for the PC.

The digital ID can also be used to encrypt other unique digital identification including account numbers, digital certificates, etc., and store the results in the protected storage of the TPM. The protected storage of the TPM is essentially non-volatile storage that has a means of access control. This access control determines which entities (e.g., user, programs, etc.) have permission to read, write, modify, and update the secure memory of the TPM. It is assumed that protected storage has some form of access control protocol that is used to protect against certain kinds of attack.

A distributed architecture of the system software enabling multiple web servers 69, each of which may host their own copy of a server 34 to communicate and interact with one or more transaction clearinghouses 30 is shown in FIG. 26. As shown in FIG. 26, there are multiple servers 69 residing in a geographically distributed manner on the Internet, each one of them with their own copy of a secure transaction server. The transaction clearinghouse 30 contains the enterprise wide account holder database, the transaction and demographics data warehouse, and controls the authentication and authorization of account holders on all the web servers 69.

When an account holder attempts to access a transaction service from any secure transaction enabled web sites, the respective server 69 for that web site will need to authenticate the account holder. In order to perform account holder

authentication, the secure transaction server will need to interact with the system transaction clearinghouse 30 by establishing and maintaining a communication line between itself and the transaction clearinghouse. The information transmitted on this communication line is encrypted using a public/private key mechanism so that only authentic servers and an authentic transaction clearinghouse can communicate with each other. The server 69 also implements the same mechanism in sending transaction data to the transaction clearinghouse's data warehouse.

The other secure transaction servers interact with the transaction clearinghouse 30 in the same manner. Thus a transaction service can host several geographically distributed secure transaction enabled web sites. Once an account holder is authenticated at one of the system enabled web sites, that account holder can access other likewise enabled web sites transparently using the same username, password, PIN combination, and the optional digital ID read from the access media by the hardware key 54, without having to again provide their username, password, PIN, and optional digital ID thus creating a single sign-on scenario where transaction services and computer resources can be accessed from a multitude of sources. All the transaction data generated by the account holder on all these different enabled web sites will be reported back to the transaction clearinghouse, regardless of how the account holder accesses the different enabled web servers 69. In the configuration of FIG. 26, the same transaction clearinghouse 30 was controlling all the secure transaction servers. However, the distributed architecture can be further extended to allow multiple secure transaction servers to interact with multiple transaction clearinghouses 30, which is shown in FIG. 27.

FIG. 27 shows multiple transaction clearinghouse two transaction clearinghouses shown), specifically a transaction clearinghouse A in Omaha and a transaction clearinghouse B in Chicago. Each transaction clearinghouse contains the business rules for account holder services, enforced by the individual transaction clearinghouse's enterprise wide account holder database. Assume that account holder "a" is registered with transaction clearinghouse A, and account holder "b" is registered with transaction clearinghouse B. Each secure transaction server 69 can provide secure transaction services for account holders from more than one transaction clearinghouse. For example, server 1 in Boston can provide secure transaction services to account holder A and account holder B even though they are registered at different transaction clearinghouses. In this case, the secure transaction server 1 in Boston is doing all the authentication, authorization and transaction data updates for account holder A through transaction clearinghouse A, and account holder B through transaction clearinghouse B. This scenario fits perfectly for a secure transaction service provider who wants to provide hosting services for several customers. The provider can run a web site with a copy of the secure transaction server, and host different transaction services through the secure transaction server, where different transaction clearinghouses are controlling different transaction services.

This also presents the possibility of transaction clearinghouses forming alliances with one another. For instance, in our example above, let's suppose transaction clearinghouse A and transaction clearinghouse B form a joint agreement that they will let each other's account holders access each other's account holder services, and each transaction clearinghouse will pay a share of the dividend to the other based on transaction volumes. In order to do this, system servers will need

to be configured to perform authentication from both transaction clearinghouses. As a result, an account holder who is registered with transaction clearinghouse A can access account holder services that fall under transaction clearinghouse B.

With regard to the case of server 1 hosting account holders A and B, since now an account holder registered with transaction clearinghouse A can also access account holder services that fall under transaction clearinghouse B, account holder "a" should be able to access account holder B through server 1. In order to do this, the server 1 will need to change its configuration so that it is able to separate transaction clearinghouse A account holders from transaction clearinghouse B account holders. When account holder "a" tries to access transaction services, secure transaction server 1 will interact with transaction clearinghouse A to do authentication, and if it is account holder "b", secure transaction server 1 will interact with transaction clearinghouse B.

However, the transaction data for a particular account holder will be sent to the transaction clearinghouse that owns the account holder. So even if account holders from transaction clearinghouse A can now access account holder B, all their transaction data will still be sent to transaction clearinghouse B. Thus, all of account holder "a" is transaction data regarding account holder B and go to transaction clearinghouse B. In this way, transaction clearinghouse B knows how many account holders from other transaction clearinghouses have accessed account holders that belong to transaction clearinghouse B, and based on that data, transaction clearinghouse B will be able to charge other transaction clearinghouses.

In accordance with another aspect of the present invention, the manner in which messages are sent among the various components will now be described in connection with the preferred embodiments of the programs that are utilized by the system. In this regard, the following is a listing of the software products that are part of the preferred embodiment of the present invention. The documents identified are specifically incorporated by reference.

#### Account Holder Database

Product: Sybase SQL Server XI

Installing Sybase SQL Server for Microsoft Windows NT  
Sybase SQL Server Release 11.0.x

Document ID: 34714-1101-02  
Last Revised Mar. 6, 1996

Introducing Sybase SQL Server for Microsoft Windows NT  
Sybase SQL Server Release 11.0.x

Document ID: 31965-1101-02  
Last Revised Feb. 10, 1996

Configuring and Administering Sybase SQL Server for Microsoft Windows NT

Sybase SQL Server Release 11.0.x  
Document ID: 36446-1101-02

Last Revised Feb. 22, 1996

Installing Sybase Products on Sun Solaris 2.x (SPARC)

Open Client/Server Release 11.1.x

Document ID: 35075-1100-03

Last Revised Sep. 10, 1996

Open Client/Server Configuration Guide for UNIX

Open Client/Server Release 11.1.x  
Document ID: 35831-1100.quadrature.02

Last Revised Aug. 21, 1996

Open Client/Server Programmer's Supplement for UNIX

Open Client/Server Release 11.1.x

Document ID: 35456-1100-04

Last Revised Aug. 23, 1996

**25**

Sybase SQL Server Utility Programs for UNIX  
 Sybase SQL Server Release 10.0  
 Document ID: 30475-01-1000-04  
 Change Level: 1  
 Last Revised Feb. 1, 1994

Sybase SQL Server System Administration Guide  
 Sybase SQL Server Release 10.0  
 Document ID: 32500-01-1000-03  
 Change Level: 3  
 Last Revised Jun. 17, 1994

Sybase SQL Server Reference Manual: Volume 1 Commands, Functions, and Topics  
 Sybase SQL Server Release 10.0  
 Document ID: 32401-01-1000-03  
 Change Level: 2  
 Last Revised Jun. 17, 1994

Sybase SQL Server Reference Manual: Volume 1 System Procedures and Catalog Stored Procedures  
 Sybase SQL Server Release 10.0  
 Document ID: 32402-01-1000-03  
 Change Level: 2  
 Last Revised Jun. 17, 1994

Sybase SQL Server 11 Unleashed  
 by Ray Rankins, Jeffrey R Garbus, David Solomon, and Bennett W McEwan  
 ISBN #0-672-30909-2  
 Library of Congress Catalog Card #95-72919  
 Sams Publishing, 201 West 103rd Street, Indianapolis, Ind. 46290  
 Copyright© 1994

Sybase Developer's Guide  
 by Daniel J Worden  
 ISBN #0-672-30467-8  
 Library of Congress Catalog Card #93-87172  
 Sams Publishing, 201 West 103rd Street, Indianapolis, Ind. 46290  
 Copyright© 1994

ODBC Driver  
 Intersolv DataDirect ODBC Drivers  
 October 1995  
 9420 Key West Avenue  
 Rockville, Md. 20850  
 MA-ODBC-211-DREF

Intersolv DataDirect ODBC Drivers Installation Guide  
 Microsoft Windows, Microsoft Windows 95, Microsoft Windows NT, and OS/2  
 October 1995  
 9420 Key West Avenue  
 Rockville, Md. 20850  
 MA-ODBC-211-INST

Intersolv ServiceDirect Handbook  
 Fourth Edition November 1995  
 Copyright© 1995  
 Intersolv, Inc.  
 9420 Key West Avenue  
 Rockville, Md. 20850  
 QCS95-S-0231

Inside ODBC by Kyle Geiger  
 ISBN #1-55615-815-7  
 Library of Congress Catalog Card #95-18867  
 Microsoft Press  
 Copyright© 1995

Server Application (Web Server)  
 Product: Netscape Enterprise Server  
 Netscape Enterprise Server Version 2.0 Administrator's Guide  
 Copyright 1996

**26**

Netscape Communications Corporation  
 501 East Middlefield Road  
 Mountain View, Calif. 94043  
 802-7610-10

5 Netscape Enterprise Server Version 2.0 Programmer's Guide  
 Copyright© 1996  
 Netscape Communications Corporation  
 501 East Middlefield Road  
 Mountain View, Calif. 94043  
 802-7611-10

10 Client Application (Web browser)  
 Product: Netscape Navigator  
 Netscape Navigator Gold Authoring Guide  
 Copyright 1996  
 15 Netscape Communications Corporation  
 501 East Middlefield Road  
 Mountain View, Calif. 94043  
 802-7612-10

20 Using Netscape  
 ISBN #0-7897-0211-8  
 Library of Congress Catalog #95-67809  
 Copyright© 1995  
 Que Corporation  
 25 201W. 103rd Street  
 Indianapolis, Ind. 46290  
 Hardware Key  
 Product: iKey 1000 Smart Token (Hardware Token)  
 Rainbow Technologies, Inc.  
 50 Technology Drive  
 Irvine, Calif. 92618  
 30 Product: Mag-Wedge Reader (Magnetic Card Reader)  
 Magtek  
 20725 South Annalee Avenue  
 Carson, Calif. 90746  
 Product: GemPC430 (Smart-Card Reader)  
 Gemplus Corporation  
 3 Lagoon Drive  
 Redwood City, Calif. 94065-1566  
 40 Product: FIU/SS2K (Fingerprint Biometric Reader)  
 Sony Electronics, Inc.  
 1 Sony Drive  
 Park Ridge, N.J. 07656-8002  
 Product: TPM (Trusted Platform Module—Secure CPU)  
 Infineon Technologies North America Corporation  
 1730 North First Street  
 San Jose, Calif. 95112  
 The secure transaction system (STS) is the preferred embodiment of the present invention in the web environment.  
 50 The following table lists the STS software components as they relate to the present invention:

---

Preferred Embodiment Component	STS software component
Transaction clearinghouse user authentication	userauthd
55 daemon	
Transaction clearinghouse transaction daemon	transactiond
Transaction clearinghouse administration	ch_admin.exe
software	
STS Server Session Manager	sessiond
STS shard object for Web server	sts.so
60 STS log-in CGI's	start_login.cgi login.cgi vrifypswd.cgi check_key.cgi verify_key.cgi
STS re-authentication CGI's	application.html application.cgi account_holder.cgi verify_applicant.cgi
STS online application CGI's and HTML	

-continued

		PARAMETER	DESCRIPTION
STS online activation CGI's	activate.cgi		
STS password change CGI's	check_activate.cgi		
STS Site Administration CGI's	pswd_chg_form.cgi	5 logdir	Absolute pathname specification of the directory which this daemon is to create its log files in. Two instances of the same daemon type (e.g., userauthd) cannot log to the same directory. The daemon will not start up if it is unable to write to the directory.
	chg_pswd.cgi		
	add_profile.cgi	10 service	Specifies the TCP port number which the daemon is to use to listen for requests. This can be a numeric or alphanumeric entry. If the entry is alphanumeric, there should be a corresponding entry in the /etc/services file.
	del_subs.cgi		
	srvconf.cgi		
	admin_subs.cgi		
	profile.cgi	15 dbserver	The name of the database server to connect to. This entry should correspond to an entry in the database server interface file.
	stadmin.cgi		
	chng_srvconf.cgi		
	data_dumprestore.cgi		
	smgr_restart.cgi	15 dname	The name of the database to use. A database server can control many databases.
	upd_profile.cgi		
	data_recovery.cgi		
	smgr_start.cgi	dbuser	The name of the database user to use when connecting to the database. Database users can be used to control what processes (or daemons) can connect to the database and also what permissions they have when they connect.
	upd_subs.cgi		
	del_profile.cgi		
	smgr_stop.cgi		
STS Account holder software	STS Client Plug-in	20	Typically all transaction clearinghouse components will use the same database server name, database name, database username and hence database user password entries in their configuration files.
	STS ActiveX component		
	dbpswd	25	The password to use for the above database user. The file permissions for this configuration should be set according knowing that it contains a database username and password.

Following is a description how these STS components can be configured, initialized, and how their day-to-day operation can be monitored. It should be understood that the component names used in these descriptions are specific to STS, and the procedures described to perform the day-to-day operation are specific to STS components, more so as an example of the preferred embodiment of the present invention in the web environment.

With respect to the configuration files that are necessary for operating the various software components of the system, each component has its own configuration file as shown below:

Daemon/Server	Configuration Filename
User Authentication	userauthd.conf
Transaction	transactiond.conf
Session Manager	sessiond.conf
Web Server	magnus.conf
	obj.conf
	mime.types

Each daemon accepts the name of its configuration file as a command line argument when starting the daemon. The format of the command line is:

<daemon name><configuration file>.

The transaction clearinghouse daemons can be started by using standard shell scripts.

For the account holder authentication daemon userauthd.conf), the following configuration files apply:

		PARAMETER	DESCRIPTION
	logdir	5	Absolute pathname specification of the directory which this daemon is to create its log files in. Two instances of the same daemon type (e.g., transactiond) cannot log to the same directory. The daemon will not start up if it is unable to write to the directory.
	service	10	Specifies the TCP port number which the daemon is to use to listen for requests. This can be a numeric or alphanumeric entry. If the entry is alphanumeric, there should be a corresponding entry in the /etc/services file.
	dbserver		The name of the database server to connect to. This entry should correspond to an entry in the database server interface file.
	dname	15	The name of the database to use. A database server can control many databases.
	dbuser		The name of the database user to use when connecting to the database. Database users can be used to control what processes (or daemons) can connect to the database and also what permissions they have when they connect.
	dbpswd	20	Typically all transaction clearinghouse components will use the same database server name, database name, database username and hence database user password entries in their configuration files.
		25	The password to use for the above database user. The file permissions for this configuration should be set according knowing that it contains a database username and password.

For the transaction daemon (transactiond.conf), the following configuration files apply:

		PARAMETER	DESCRIPTION
	logdir	35	Absolute pathname specification of the directory which this daemon is to create its log files in. Two instances of the same daemon type (e.g., transactiond) cannot log to the same directory. The daemon will not start up if it is unable to write to the directory.
	service	40	Specifies the TCP port number which the daemon is to use to listen for requests. This can be a numeric or alphanumeric entry. If the entry is alphanumeric, there should be a corresponding entry in the /etc/services file.
	dbserver		The name of the database server to connect to. This entry should correspond to an entry in the database server interface file.
	dname	45	The name of the database to use. A database server can control many databases.
	dbuser		The name of the database user to use when connecting to the database. Database users can be used to control what processes (or daemons) can connect to the database and also what permissions they have when they connect.
	dbpswd	50	Typically all transaction clearinghouse components will use the same database server name, database name, database username and hence database account holder password entries in their configuration files.
		55	The password to use for the above database user. The file permissions for this configuration should be set according knowing that it contains a database username and password.

For the session manager (sessiond.conf), the following configuration files apply:

Parameter	Description
SESSIOND_UDP_PORT	Specifies the UDP port which the session manager will use to list for requests from CGI programs.
SESSIOND_TCP_PORT	Specifies the TCP port which the session manager will use to listen for replies from the transaction clearinghouse.

-continued

Parameter	Description
TRANSACTION_CLEARINGHOUSE_HOST	The UNIX host name that the transaction clearinghouse server is running on. When the session manager communicates with the transaction clearinghouse, this entry forms part of the address.
TRANSACTION_CLEARINGHOUSE_PORT	This entry specifies the TCP port which the session manager should use when communicating with the transaction clearinghouse transaction daemon. The session manager uses this entry and the TRANSACTION CLEARINGHOUSE_HOST entry to build the complete address for the transaction daemon. This port number should match the port number defined in the service entry of the transaction daemons configuration file.
TRANSACTION_CLEARINGHOUSE_URL_PORT	This entry specifies the TCP port which the session manager should use when communicating with the transaction clearinghouse URL tracking daemon. The session manager uses this entry and the TRANSACTION CLEARINGHOUSE_HOST entry to build the complete address for the URL tracking daemon. This port number should match the port number defined in the service entry of the URL tracking daemons configuration file.
TRANSACTION_CLEARINGHOUSE_AUTH_PORT	This entry specifies the TCP port that the session manager should use when communicating with the transaction clearinghouse account holder authentication daemon. The session manager uses this entry and the TRANSACTION CLEARINGHOUSE_HOST entry to build the complete address for the account holder authentication daemon. This port number should match the port number defined in the service entry of the account holder authentication daemons configuration file.
COMPANY_NO	Unique ID assigned to each company defined with the secure transaction server system.
ACCOUNT HOLDER_ID	Unique ID assigned to each account holder defined for a company in the secure transaction server system.
KEYCHECK_INTERVAL	The number of seconds that will elapse before the secure transaction server asks the browser to check for the existence of the access device.
REFRESH_TIME	The amount of time (in seconds) that must expire without any session activity before a session is considered inactive and terminated.
SESSION_REFRESH_INTERVAL	The amount of time (in seconds) that must elapse with no new connection requests to the secure transaction server, which will cause the secure transaction server to stop listening for incoming connections and go examine its internal session table to see if any sessions have become idle (refresh time has expired for the session). It will clean up idle sessions and resume listening for incoming connection requests.
LOCAL_TRANSACTION_TRACK	Indicates if the transaction tracking data is stored locally as well as being sent to the transaction clearinghouse for storage. Valid entries are YES or NO.
MAX_RESEND_NO	If the secure transaction server does not get a confirmation message back from the transaction clearinghouse for information it sent to the secure access transaction clearinghouse, the secure transaction server will resend the data until we get a confirmation message or until the maximum times to resend transaction data has been exceeded.
ADMIN_EMAIL_ADDR	When an event occurs that requires intervention from an administrator, notification is sent to this email address.
MAIL_BIN	Absolute filename specification of the program to use to send email notification to the person defined in ADMIN_EMAIL_ADDR.

-continued

Parameter	Description
TRANSACTION	This defines the granularity of the transaction data that the session manager records about a session. There are two valid entries: SESSION or TRAN. TRAN indicates that the session manager should record information about every transaction that occurred in a session. SESSION indicates that only information regarding the session should be stored, i.e., session start and end times, account holder ID, number of transactions that occurred in session manager.
LOCAL_AUTHENTICATION	Indicates if account holder authentication should be performed against a local database as opposed to the transaction clearinghouse database. Valid entries are YES or NO. YES indicates that authentication should be performed locally, while NO indicates the opposite.
RUNTIME_DIR	This is the default directory for the secure transaction server. Here is where the secure transaction server will create log files and other dynamic run time files required for successful operation.

For the web server (magnus.conf), in order that the system shared object 66 component works correctly with the web server, the following changes need to be made to the magnus.conf file:

---

```
# load the account holderaccount holder access specific NSAPI functions
#
Init fn=load-modules shlib=/usr/ns-home/bin/load_modules/sts.so
funcs=init-sts,restrict-by-sts,log-end,restrict-by-rpa
#
#call init-sts to initialize sts server specific NSAPI
#variables
#
Init fn=init-sts
Sm_host=localhost
login_url=http://10.199.199.7/cgi-bin/gatekpr/login.cgi
keycheck_url=http://10.199.199.7/cgi-bin/gatekpr/check_key.cgi
smerr_url=http://10.199.199.7/gatekpr/session_err.html
```

---

It should be noted that all the <variable><value> pairs listed above should appear on the line beginning Init if and should be separated with spaces. Each variable/pair value was listed on a separate line to aid clarity.

The following describes the meaning of each of NSAPI variables:

Sm\_host: hostname or the IP address of the machine hosting session manager daemon(s)

login\_url: URL for the account holderaccount holder access login CGI

keycheck\_url: URL for account holderaccount holder access re-authentication CGI

smerr\_url: URL for error HTML for session manager errors (configurable)

For the web server (obj.conf), for each directory protected by the secure transaction system, the following entries need to be inserted in obj.conf:

---

```
<Object ppath="/usr/ns-home/htdocs_unsecure/demosite/*">
PathCheck fn="restrict-by-sts"
log_head="prism_login.txt"
session_port="50420"
trailer="prism_tail.txt"
err_head="prism_err.txt"
digest="S"
AddLog fn="log-end"
</Object>
```

---

Once again, each entry was placed on a separate line for clarity but when adding them to the configuration file all the entries should be on the same line, separated by spaces.

25 The variable meaning is as follows:

log\_head: text file containing the HTML header tags for the login page

session\_port: session manager's port number

30 trailer: text file containing the HTML trailer tags for login page and error pages

err\_head: text file containing the HTML header tags for error pages

digest: message digest type to use for one-time-password encryption (4-MD4; 5-MD5)

35 For the web server configuration file (mime.types), one line needs to be added to the mime.types configuration file. The line is:

type=application/x-protect exts=pro

40 The positioning of the new line within the configuration file is not important. Adding this line enables any file with the extension pro to automatically invoke the client side software to process the file.

With respect to routine operating procedures, there are 45 general guidelines for the orderly start up and shutdown of the system of the present invention. To start up the system, there are a sequence of activities that are involved. First, each server should be configured through its configuration files. Each of the transaction clearinghouse servers is started by a series of

50 shell strips, which in a typical installation, will be in the directory named /usr/local/sts/transaction clearinghouse. The /usr/local part of the previous pathname was the directory specified at installation time. The scripts are named start\_userauthd.sh, start\_transactiond.sh and start\_urltrackd.sh. After the scripts are executed, the PS-EF command is used to check if the following processes exist: userauthd, transactiond and urltrackd. The next step is to start up the database server which requires login as the account holder sysbase. This login will have an environment variable called

55 SYBASE which defines what directory SYBASE was installed to. It is necessary to move to the directory SSYBASE/bin. For each database server to be started, there is a file called RUN\_<SERVER\_NAME>. If two database servers called STS and STS\_backup were created during the installation, the start up files would be called RUN\_STS and RUN\_STS\_BACKUP. This start up file should be used in conjunction with the startserver program. The exact syntax is:

33

startserver {-f<startup files>}. To continue the example from above, the command would be: startserver -f RUN\_STS-f RUN\_STS\_BACKUP.

With respect to the session manager, it can be started by a shell script and there will be one instance of the session manager per account holder per company. If the installation directory was specified to be /usr/local then the session manager start up scripts will be found at /usr/local/STS/sessionmgr. The naming convention for the start up scripts is: start\_<account holder name>.sh. Each account holder will have its own directory off of /usr/local/STS/sessionmgr.

With respect to the web server, once its configuration files have been modified as indicated above, the account holder access component will automatically be used once the web server is started. As web servers from different vendors require different start up procedures, it is assumed that this information is already known.

With respect to shutdown, of the system and particularly the web server, it is best to start with the secure transaction server as this is the first point of contact for the account holder's browser. Like the start up procedure for the web server, the shutdown procedure will differ for each different web server.

With respect to the session manager, it is recommended that shutdown of it be done from within the server side administration program. The browser should be pointed at the URL where the server site administration program is located and the administer button for the session manager that is wanted to be stopped should be clicked. A data dump on the session manager should be performed before stopping it to avoid loss of data contained within the manager to be stopped. This is executed by entering the complete pathname of the data dump file and clicking the data dump button. With respect to the transaction clearinghouse, the transaction clearinghouse daemons are shutdown using the kill command. The process identification numbers for each of the servers should be found by getting a list of all processes and searching for the process names of the start up procedures. Once the process identification numbers have been established, the command kill -9 <pid>{<pid>} should be used.

With respect to the database server, it can be shutdown using the following steps:

```

login into isql as the system administrator
type "shutdown <backup database server name>"
type "go"
type "shutdown"
type "go"
hadji:>isql -Usa -P -SSTS
1> shutdown SYB BACKUP
2> go
Backup Server: 3.48.1.1: The Backup Server will go down
immediately.

Terminating sessions.
1> shutdown
2> go
Server SHUTDOWN by request.
The SQL Server is terminating this process.
00:97/05/14 14:52:40.23 server SQL Server shutdown by
request.
00:97/05/14 14:52:40.24 kernel ushutdown: exiting DB-
LIBRARY error:
Unexpected EOF from SQL Server.
hadji:>

```

It should be understood from the foregoing that a secure transaction system has been shown and described which enables a business to have total control over account holder access, transaction tracking and billing over an untrusted

34

network such as the Internet world wide web. The system has many desirable attributes and features that Enable it to provide such functionality. Moreover, it is extremely flexible in that it can operate to function with multiple servers and multiple transaction clearinghouses if desired. Moreover, two-factor authentication enables the system to frequently determine if a account holder is authentic and the system also functions to authenticate servers as well. A secure platform for businesses to securely provide transaction services to the world wide web in a way that assures revenue generation if that is a goal is a prominent feature of the system of the present invention.

While various embodiments of the present invention have been shown and described, it should be understood that other modifications, substitutions and alternatives are apparent to one of ordinary skill in the art. Such modifications, substitutions and alternatives can be made without departing from the spirit and scope of the invention, which should be determined from the appended claims.

Other embodiments of the invention will be apparent to those skilled in the art from consideration of the specification and practice of the invention disclosed herein. It is intended that the specification and examples be considered as exemplary only, with a true scope and spirit of the invention being indicated by the following claims.

We claim:

1. A system for controlling access to protected computer resources provided via a network utilizing at least one Internet Protocol, the system comprising:

at least one authentication server having an associated database to store (i) identity data associated with at least one client computer device, and (ii) data associated with said protected computer resources;

at least one access server adapted to receive said identity data from said at least one client computer device;

said at least one access server adapted to forward said identity data received from said at least one client computer device to said at least one authentication server;

said at least one authentication server adapted to authenticate said identity data responsive to a request for said protected computer resources by said at least one client computer device;

said at least one authentication server adapted to authorize said at least one client computer device to receive at least a portion of said protected computer resources, based on said stored data associated with said protected computer resources; and

said at least one authentication server adapted to permit access to said at least a portion of said protected computer resources upon successfully authenticating said identity data and upon successfully authorizing said at least one client computer device.

2. The system of claim 1, wherein said identity data is one of derived and generated from at least one internal hardware component of said at least one client computer device.

3. The system of claim 1, wherein said identity data is one of derived and generated from at least a portion of a plurality of hardware components of said at least one client computer device.

4. The system of claim 1, wherein said identity data is one of derived and generated from one of an external device and an external object connected to said at least one client computer device.

5. The system of claim 4, wherein said one of an external device and an external object is a subscriber identity module.

6. The system of claim 1, wherein said identity data is one of derived and generated from one of an external device and

an external object inserted into a reader associated with said at least one client computer device.

7. The system of claim 6, wherein said one of an external device and an external object is a subscriber identity module.

8. The system of claim 1, wherein said identity data associated with said at least one client computer device comprises a digital certificate.

9. The system of claim 1, wherein at least a portion of said identity data associated with said at least one client computer device is encrypted.

10. The system of claim 1, wherein said identity data associated with said at least one client computer device contains at least one hash value.

11. The system of claim 1, wherein said at least one client computer device is adapted to authenticate said at least one access server.

12. The system of claim 1, wherein said at least one access server is adapted to receive said identity data associated with said at least one client computer device and at least one of a username and a password.

13. The system of claim 1, wherein said at least one access server is adapted to receive said identity data associated with said at least one client computer device via a network utilizing at least one Internet Protocol.

14. The system of claim 1, wherein said identity data associated with said at least one client computer device is forwarded to said at least one access server.

15. The system of claim 1, wherein said identity data associated with said at least one client computer device is known in advance.

16. The system of claim 1, wherein said identity data associated with said at least one client computer device is unique to said at least one client computer device.

17. The system of claim 1, wherein said identity data associated with said at least one client computer device is unique to a group of client computer devices comprising said at least one client computer device.

18. The system of claim 1, wherein said data associated with said protected computer resources is stored in a database of at least one server computer associated with said at least one authentication server.

19. The system of claim 1, wherein said at least the portion of said protected computer resources are provided via a network utilizing at least one Internet Protocol to said at least one client computer device by at least one server computer associated with said at least one access server upon said at least one authentication server permitting access to said at least the portion of said protected computer resources.

20. The system of claim 1, wherein said at least the portion of said protected computer resources are stored in at least one of a plurality of server computers associated with said at least one access server.

21. The system of claim 1, wherein said at least the portion of said protected computer resources are stored in a database associated with said at least one access server.

22. The system of claim 1, wherein at least one of a plurality of server computers associated with said at least one access server is adapted to provide said at least the portion of said protected computer resources to said at least one client computer device upon said at least one authentication server permitting access to said at least the portion of said protected computer resources.

23. The system of claim 1, wherein said at least a portion of said protected computer resources is encrypted.

24. The system of claim 1, wherein said at least one authentication server is located on a computer separate from said at least one access server.

25. The system of claim 1, wherein said at least one authentication server is located on the same computer as said at least one access server.

26. The system of claim 1, wherein at least one of the functions of said at least one authentication server are performed by another server associated with said at least one authentication server.

27. The system of claim 1, wherein said at least one authentication server is adapted to authenticate multiple client computer devices.

28. The system of claim 1, wherein said at least one authentication server is adapted to authenticate multiple access servers.

29. The system of claim 1, wherein said at least one authentication server is one of a plurality of servers adapted to authenticate.

30. The system of claim 1, wherein said at least one authentication server is one of a plurality of servers adapted to authorize.

31. The system of claim 1, wherein said at least one authentication server is one of a plurality of servers adapted to permit access.

32. The system of claim 1, wherein said authentication server is adapted to assign one of a plurality of authorization levels to said at least a portion of said protected computer resources, is adapted to assign a particular authorization level to said identity data associated with said at least one client computer device, and is adapted to only permit access to particular protected computer resources by said at least one client computer device permitted by said particular authorization level.

33. The system of claim 1, wherein said at least one access server is adapted to selectively require said at least one client computer device to forward said identity data associated with said at least one client computer device to said at least one access server.

34. The system of claim 1, wherein said at least one access server is adapted to selectively prompt said at least one client computer device to provide said identity data associated with said at least one client computer device and at least one of a username and a password to said at least one access server.

35. The system of claim 1, wherein said at least one access server is adapted to selectively query said at least one client computer device to one of derive and generate said identity data associated with said at least one client computer device.

36. The system of claim 1, wherein said at least one access server is adapted to change said identity data associated with said at least one client computer device, and to forward said changed identity data to said at least one authentication server.

37. The system of claim 1, wherein at least one of said at least one access server and a server associated with said at least one authentication server is adapted to acquire, for billing purposes, usage data of said at least a portion of said protected computer resources provided to said at least one client computer device.

38. A system for controlling access to protected computer resources provided via a network utilizing at least one Internet Protocol, the system comprising:

at least one authentication server having an associated database to store (i) identity data of at least one access server, (ii) identity data associated with at least one client computer device, and (iii) data associated with said protected computer resources;  
said at least one access server adapted to receive said identity data from said at least one client computer device;

said access server adapted to forward said identity data of said at least one access server and said identity data associated with said at least one client computer device received from said at least one client computer device to said at least one authentication server;  
 said at least one authentication server adapted to authenticate said identity data of said at least one access server and said identity data associated with said at least one client computer device responsive to a request for said protected computer resources by said at least one client computer device;  
 said at least one authentication server adapted to authorize said at least one client computer device to receive at least a portion of said protected computer resources, based on said stored data associated with said protected computer resources; and  
 said at least one authentication server adapted to permit access to said at least said portion of said protected computer resources upon successfully authenticating said identity data of said access server and said identity data associated with said at least one client computer device, and upon successfully authorizing said at least once client computer device.

**39.** The system of claim **38**, wherein said identity data is one of derived and generated from at least one internal hardware component of said at least one client computer device.

**40.** The system of claim **38**, wherein said identity data is one of derived and generated from at least a portion of a plurality of hardware components of said at least one client computer device.

**41.** The system of claim **38**, wherein said identity data is one of derived and generated from one of an external device and an external object connected to said at least one client computer device.

**42.** The system of claim **41**, wherein said one of an external device and an external object is a subscriber identity module.

**43.** The system of claim **38**, wherein said identity data is one of derived and generated from one of an external device and an external object inserted into a reader associated with said at least one client computer device.

**44.** The system of claim **43**, wherein said one of an external device and an external object is a subscriber identity module.

**45.** The system of claim **38**, wherein said identity data associated with said at least one client computer device comprises a digital certificate.

**46.** The system of claim **38**, wherein at least a portion of said identity data associated with said at least one client computer device is encrypted.

**47.** The system of claim **38**, wherein said identity data associated with said at least one client computer device contains at least one hash value.

**48.** The system of claim **38**, wherein said at least one client computer device is adapted to authenticate said at least one access server.

**49.** The system of claim **38**, wherein said at least one access server is adapted to receive said identity data associated with said at least one client computer device and at least one of a username and a password.

**50.** The system of claim **38**, wherein said at least one access server is adapted to receive said identity data associated with said at least one client computer device via a network utilizing at least one Internet Protocol.

**51.** The system of claim **38**, wherein said identity data is forwarded to said at least one access server.

**52.** The system of claim **38**, wherein said identity data associated with said at least one client computer device is known in advance.

**53.** The system of claim **38**, wherein said identity data associated with said at least one client computer device is unique to said at least one client computer device.

**54.** The system of claim **38**, wherein said identity data associated with said at least one client computer device is unique to a group of client computer devices comprising said at least one client computer device.

**55.** The system of claim **38**, wherein said data associated with said protected computer resources is stored in a database of at least one server computer associated with said at least one authentication server.

**56.** The system of claim **38**, wherein said at least the portion of said protected computer resources are provided via a network utilizing at least one Internet Protocol to said at least one client computer device by at least one server computer associated with said at least one access server upon said at least one authentication server permitting access to said at least the portion of said protected computer resources.

**57.** The system of claim **38**, wherein said at least the portion of said protected computer resources are stored in at least one of a plurality of server computers associated with said at least one access server.

**58.** The system of claim **38**, wherein said at least the portion of said protected computer resources are stored in a database associated with said at least one access server.

**59.** The system of claim **38**, wherein at least one of a plurality of server computers associated with said at least one access server is adapted to provide said at least the portion of said protected computer resources to said at least one client computer device upon said at least one authentication server permitting access to said at least the portion of said protected computer resources.

**60.** The system of claim **38**, wherein said at least a portion of said protected computer resources is encrypted.

**61.** The system of claim **38**, wherein said at least one authentication server is located on a computer separate from said at least one access server.

**62.** The system of claim **38**, wherein said at least one authentication server is located on the same computer as said at least one access server.

**63.** The system of claim **38**, wherein at least one of the functions of said at least one authentication server are performed by another server associated with said at least one authentication server.

**64.** The system of claim **38**, wherein said at least one authentication server is adapted to authenticate multiple client computer devices.

**65.** The system of claim **38**, wherein said at least one authentication server is adapted to authenticate multiple access servers.

**66.** The system of claim **38**, wherein said at least one authentication server is one of a plurality of servers adapted to authenticate.

**67.** The system of claim **38**, wherein said at least one authentication server is one of a plurality of servers adapted to authorize.

**68.** The system of claim **38**, wherein said at least one authentication server is one of a plurality of servers adapted to permit access.

**69.** The system of claim **38**, wherein said authentication server is adapted to assign one of a plurality of authorization levels to said at least a portion of said protected computer resources, is adapted to assign a particular authorization level to said identity data associated with said at least one client computer device, and is adapted to only permit access to

**39**

particular protected computer resources by said at least one client computer device permitted by said particular authorization level.

**70.** The system of claim **38**, wherein said at least one access server is adapted to selectively require said at least one client computer device to forward said identity data associated with said at least one client computer device to said at least one access server.

**71.** The system of claim **38**, wherein said at least one access server is adapted to selectively prompt said at least one client computer device to provide said identity data associated with said at least one client computer device and at least one of a username and a password to said at least one access server.

**72.** The system of claim **38**, wherein said at least one access server is adapted to selectively query said at least one client computer device to one of derive and generate said identity data associated with said at least one client computer device.

**73.** The system of claim **38**, wherein said at least one access server is adapted to change said identity data associated with said at least one client computer device, and to forward said changed identity data to said at least one authentication server.

**74.** The system of claim **38**, wherein at least one of said at least one access server and a server associated with said at least one authentication server is adapted to acquire, for billing purposes, usage data of said at least a portion of said protected computer resources provided to said at least one client computer device.

**75.** A system for controlling access to protected computer resources provided via a network utilizing at least one Internet Protocol, the system comprising:

at least one authentication server having an associated database to store (i) identity data of at least one access server, (ii) identity data of a subscriber identity module associated with at least one client computer device, and (iii) authorization data associated with said protected computer resources;

said at least one authentication server adapted to register said identity data of a subscriber identity module associated with said at least one client computer device; said at least one access server adapted to receive (i) said identity data of a subscriber identity module associated with said at least one client computer device and (ii) a request for said protected computer resources from said at least one client computer device;

said at least one client computer device adapted to receive an acknowledgement for said request for said protected computer resources from said at least one access server; said at least one access server adapted to forward (i) said identity data of said at least one access server and (ii) said identity data of a subscriber identity module received from said at least one client computer device to said at least one authentication server;

said at least one authentication server adapted to authenticate (i) said identity data of said at least one access server and (ii) said identity data of a subscriber identity module associated with said at least one client computer device responsive to a request for said protected computer resources by said at least one client computer device; said at least one authentication server adapted to authorize

said at least one client computer device to receive at least a portion of said protected computer resources, based on said stored authorization data associated with said protected computer resources;

said at least one authentication server adapted to permit access to said at least said portion of said protected computer resources (i) upon successfully authenticating

**40**

said identity data of said access server and said identity data of a subscriber identity module associated with said at least one client computer device, and (ii) upon successfully authorizing said at least one client computer device;

at least one of said at least one access server and a server associated with said at least one authentication server adapted to acquire, for billing purposes, usage data of said at least a portion of said protected computer resources provided to said at least one client computer device; and

said at least one authentication server adapted to re-authenticate said identity data of a subscriber identity module associated with said at least one client computer device.

**76.** The system of claim **75**, wherein said at least one client computer device is adapted to authenticate said at least one access server.

**77.** The system of claim **75**, wherein said at least one access server is adapted to receive said identity data of a subscriber identity module associated with said at least one client computer device and at least one of a username and a password.

**78.** The system of claim **75**, wherein said at least one access server is adapted to receive said identity data of a subscriber identity module associated with said at least one client computer device via a network utilizing at least one Internet Protocol.

**79.** The system of claim **75**, wherein the storing of said authorization data associated with said protected computer resources is stored in a database of at least one server computer associated with said at least one authentication server.

**80.** The system of claim **75**, wherein said at least the portion of said protected computer resources are provided via a network utilizing at least one Internet Protocol to said at least one client computer device by at least one server computer associated with said at least one access server upon said at least one authentication server permitting access to said at least the portion of said protected computer resources.

**81.** The system of claim **75**, wherein said at least the portion of said protected computer resources are stored in at least one of a plurality of server computers associated with said at least one access server.

**82.** The system of claim **75**, wherein said at least the portion of said protected computer resources are stored in a database associated with said at least one access server.

**83.** The system of claim **75**, wherein at least one of a plurality of server computers associated with said at least one access server is adapted to provide said at least the portion of said protected computer resources to said at least one client computer device upon said at least one authentication server permitting access to said at least the portion of said protected computer resources.

**84.** The system of claim **75**, wherein said at least a portion of said protected computer resources is encrypted.

**85.** The system of claim **75**, wherein said at least one authentication server is located on a computer separate from said at least one access server.

**86.** The system of claim **75**, wherein said at least one authentication server is located on the same computer as said at least one access server.

**87.** The system of claim **75**, wherein at least one of the functions of said at least one authentication server are performed by another server associated with said at least one authentication server.

**88.** The system of claim **75**, wherein said at least one authentication server is adapted to authenticate multiple client computer devices.

89. The system of claim 75, wherein said at least one authentication server is adapted to authenticate multiple access servers.

90. The system of claim 75, wherein said at least one authentication server is one of a plurality of servers adapted to authenticate.

91. The system of claim 75, wherein said at least one authentication server is one of a plurality of servers adapted to authorize.

92. The system of claim 75, wherein said at least one authentication server is one of a plurality of servers adapted to permit access.

93. The system of claim 75, wherein said authentication server is adapted to assign one of a plurality of authorization levels to said at least a portion of said protected computer resources, is adapted to assign a particular authorization level to said identity data associated with said at least one client computer device, and is adapted to only permit access to particular protected computer resources by said at least one client computer device permitted by said particular authorization level.

94. The system of claim 75, wherein said at least one access server is adapted to selectively require said at least one client computer device to forward said identity data associated with said at least one client computer device to said at least one access server.

95. The system of claim 75, wherein said at least one access server is adapted to selectively prompt said at least one client computer device to provide said identity data associated with said at least one client computer device and at least one of a username and a password to said at least once access server.

96. The system of claim 75, wherein said at least one access server is adapted to selectively query said at least one client computer device to one of derive and generate said identity data associated with said at least one client computer device.

97. The system of claim 75, wherein said at least one access server is adapted to change said identity data associated with said at least one client computer device, and to forward said changed identity data to said at least one authentication server.

\* \* \* \* \*